Benutzerhandbuch

Version 6.6

Impressum

iKu Systemhaus AG
Am Römerkastell 4
D-66121 Saarbrücken

Tel.: +49 (0) 6 81 / 9 67 51 - 0
Fax: +49 (0) 6 81 / 9 67 51 - 66
E-Mail: info@iku-ag.de

Technischer Support (Montag-Freitag 9-17h):

Tel.: 900 - 1/ SPONTS
77 66 87

Die kostenpflichtige Telefonnummer des Technischen Supports ist nicht über Mobiltelefone oder aus dem Ausland erreichbar.

Hinweise zu Marken

SPONTS ist ein eingetragenes Warenzeichen der iKu Systemhaus AG. Kopie, Reproduktion oder Duplikation als Ganzes oder in Teilen ist ohne ausdrückliche Erlaubnis der IKU Systemhaus AG verboten.

Microsoft, Windows und das Windows-Logo sind eingetragene Marken der Marken von Microsoft Corporation und den USA und/oder anderen Ländern.

UNIX® ist ein eingetragene Warenzeichen der Open Group.

Netscape, Netscape Navigator und Netscape Communicator sind eingetragene Warenzeichen und Dienstleistungsbezeichnungen von Netscape Communications Corporation in den USA und anderen Ländern.

Netscape Logos und die Produkt- und Dienstleistungsbezeichnungen von Netscape sind ebenfalls Warenzeichen non Netscape Communications Corporation, die in anderen Ländern eingetragen sein können.

Firefox und die Firefox Logos sind Warenzeichen der Mozilla Foundation.

Mozilla und die Mozilla Logos sind Warenzeichen der Mozilla Foundation.

Sonstige hier nicht aufgeführten Namen und Produktbezeichnungen sind möglicherweise eingetragene Marken oder Marken der betreffenden Firmen.

Inhaltsverzeichnis

1 Einführung

Herzlichen Glückwunsch, dass Sie sich für SPONTS entschieden haben. Dieses Qualitätsprodukt garantiert höchste Sicherheit für Ihre E-Mailversorgung. SPONTS ist das ideale Mittel, um die ständige Verfügbarkeit von E-Mails sicherzustellen und gleichzeitig unerwünschte Nachrichten abzuwehren.

SPONTS ist sehr einfach zu installieren und zu benutzen. Da SPONTS aber auch eine Fülle von Möglichkeiten bietet, sollten Sie dieses Handbuch aufmerksam lesen, damit dem erfolgreichen Einsatz von SPONTS nichts mehr im Wege steht.

2 Grundbegriffe

Solche Kästen enthalten Tipps und Hinweise zur Verwendung von SPONTS.

Solche Kästen enthalten Kurzbeschreibungen, die die wichtigsten Punkte zusammenfassen.

2.1 MX (Mail-Exchanger)

Ein *MX* ist der für eine Internet-Domain zuständige Mailserver. Im *Domain Name Service* (DNS) ist für jede Domain vermerkt, welcher Mailserver Nachrichten für diese annimmt. Hierbei können mehrere Server mit gleicher oder unterschiedlicher Priorität angegeben werden. Beim Verschicken einer Mail an diese Domain wird zuerst der Server mit der niedrigsten Priorität kontaktiert. Ist dieser nicht erreichbar, werden die anderen in aufsteigender Priorität kontaktiert. Es ist erlaubt, mehreren Servern die gleiche Priorität zu geben, um eine automatische Lastverteilung zu erreichen. Ist für eine Domain kein MX-Server eingetragen, so wird nach einer IP-Adresse (A-Eintrag) gesucht und wenn vorhanden diese kontaktiert.

Manche Spammer ignorieren die Prioritäten oder verschicken trotz vorhandenem MX-Eintrag an die Adresse im A-Eintrag. Dies hat zur Folge, dass die eigenen Server (bzw. die des eigenen Providers) Spam an den SPONTS weiterleiten. Damit diese Server von SPONTS nicht blockiert werden, sollten sie in die Whitelist (vgl. 7.3.6 Envelope, S. 58ff.) aufgenommen werden. Dies gilt auch für einen Backup-MX, da dieser einer SPF-Überprüfung nicht standhält.

2.2 Backend

Das *Backend* ist der Mailserver, an den eingehende Mail weiter geschickt werden soll. Dies kann der zuständige Mailserver (z.B. Lotus Notes, Postfix, Sendmail oder Exchange) sein, oder ein ihm vorgeschalteter Virenscanner (z.B. VirusWall).

2.3 Absendeserver

Der Server, der per SMTP eine Mail an Sie schicken will.

2.4 SMTP (Simple Mail Transfer Protocol)

SMTP ist die „Sprache“, mit der Mailserver im Internet untereinander kommunizieren. Zum Versenden einer Nachricht kontaktiert der Absendeserver den zuständigen Mailserver auf TCP-Port 25. Die Übermittlung geschieht in mehreren Schritten, in denen nacheinander der Absender, ein oder mehrere Empfänger und der Nachrichtentext übertragen werden.

3 Software-Installation

Dieses Kapitel ist nur relevant, wenn Sie SPONTS als installierbares Software-Paket erhalten haben. Wenn Sie eine SPONTS-Appliance erworben haben, ist die erforderliche Software bereits vollständig auf der gelieferten Hardware vorhanden und Sie können direkt weiterlesen auf Seite 8, Kapitel 4: Einrichtung.

3.1 Installationsvoraussetzungen

SPONTS benötigt etwa 20 MB Speicherplatz für den Programmcode, etwa 300MB für seine Daten, wobei dies von der speziellen Konfiguration abhängt und etwa 128-256 MB Hauptspeicher. Außerdem wird eine aktuelle Java-Runtime (JRE) in der Version 1.5 oder höher benötigt.

3.2 Installation von Java

Das aktuelle JRE erhalten Sie unter http://www.java.com/ bzw. von Ihrem Betriebssystem-Hersteller. Sollten Sie sich für den Download von java.com entscheiden, so ist es ausreichend, das Paket in ein Verzeichnis zu installieren und dieses bei der Konfiguration des SPONTS weiter unten anzugeben. Auf diese Weise können Sie auch ein JRE zur ausschließlichen Verwendung durch den SPONTS installieren, wenn Sie keine Veränderungen an einer bestehenden Java-Installation vornehmen wollen.

Stellen Sie nach der Installation sicher, dass die korrekte Java-Version installiert ist. Sie öffnen dazu am besten ein Kommandozeilen-Fenster und geben ein:

```
cd <bin-Verzeichnis der Java-Installation>

./java -version (unter Unix-Systemen)
java -version   (unter Windows)
```

Die Ausgabe sollte ungefähr wie folgt aussehen. Wichtig ist, dass die Version mindestens 1.5.x ist:

```
java version "1.5.0_06"
Java(TM) 2 Runtime Environment, Standard Edition (build 1.5.0_06-b05)
Java HotSpot(TM) Client VM (build 1.5.0_06-b05, mixed mode, sharing)
```

Falls das bin-Verzeichnis ihrer Java-Installation im Systempfad ('PATH') enthalten ist, müssen Sie nicht in das Verzeichnis wechseln sondern können den java-Befehl direkt verwenden.

3.3 Installer für Windows

SPONTS ist für Windows als Installer-Paket verfügbar. Führen Sie den Installer aus und folgen Sie den Anweisungen am Bildschirm.

3.4 Systemunabhängiger Installer (jar)

SPONTS ist für alle Java-fähigen Betriebssysteme mittels des Installer-Pakets im Jar-Format installierbar. Führen Sie den Installer mittels

```
java -jar <Pfad zur Jar-Datei>
```

aus und folgen Sie den Anweisungen am Bildschirm.

3.5 Installation als Paket unter Linux

Die Software-Version von SPONTS ist als Debian-Paket (DEB), als RPM-Paket für SUSE und RedHat sowie als TAR-Archiv verfügbar.

Sie müssen das Paket als Systemverwalter installieren. Beachten Sie hierzu die Hinweise Ihres Betriebssystemherstellers. Unverbindlich hier ein paar Beispielsbefehle:

Installation des Debian-Paketes

Installieren Sie das Paket mit dem Befehl

```
dpkg -i <Dateiname.deb>
```

Installation des RPM-Paketes

Installieren Sie das Paket mit dem Befehl

```
rpm -hiv <Dateiname.rpm>
```

Installation des TAR-Archives

Entpacken Sie das Paket mit dem Befehl

```
cd /; tar xvzf <Dateiname.tar.gz>
```

3.5.1 Konfiguration

Wenn Sie Java nicht systemweit installiert haben, müssen Sie SPONTS das Installationsverzeichnis des JRE mitteilen. Am einfachsten geht es, indem Sie den entsprechenden Eintrag JAVA_HOME in `/opt/sponts/conf/settings` anpassen:

```
SPONTS_USER=sponts
JAVA_HOME=/opt/jre
SPONTS_JVM_ARGS="-server -Xms32M -Xmx256M"
```

In dieser Datei können Sie auch den zu verwendenden Benutzer und die maximalen Speichernutzung von SPONTS über die Option '-Xmx' angeben. Als Suffix dürfen Sie hier 'K' für KiB und 'M' für MiB verwenden. Lassen Sie ihn weg, so wird der Wert als Byteangabe interpretiert (und 256 Byte sind zu wenig).

> WICHTIG: Standardmäßig wird SPONTS als Benutzer `sponts` gestartet, d.h. ohne root-Rechte. Damit ist es normalerweise nicht möglich, einen Dienst auf einem Port unterhalb von 1024 laufen zu lassen. Wenn Sie SPONTS auf dem Port 25 (SMTP) konfigurieren wollen, müssen Sie ihn entweder als `root` laufen lassen, einen Port-Forwarder oder unter Linux AccessFS verwenden.

Danach muss der SPONTS über das Konfigurationsskript eingerichtet werden:

```
sh /opt/sponts/bin/setup-sponts.sh
```

Die Konfiguration erfolgt in 6 Schritten:

1. Create / Overwrite all SPONTS settings?: sollen die SPONTS-Einstellungen erzeugt / überschrieben werden? Antworten Sie bei der Erstinstallation mit 'Yes', damit die Konfigurationsdatei erzeugt wird.

2. Passwort für SPONTS SQL Benutzer: SPONTS verwendet eine eigene SQL-Datenbank für seine Programm- und Logdaten. Auf diese Datenbank können Sie als Administrator auch zugreifen. Geben Sie hier 2x das Passwort an, mit dem der Zugriff erfolgen darf.
3. Passwort für SPONTS/Monitor SQL Benutzer: Die Datenbank für TKÜV ist von der normalen Datenbank getrennt, da Änderungen ausschließlich über die SPONTS-Oberfläche erfolgen dürfen. Geben Sie hier 2x das Passwort an, das diese Datenbank schützt.
4. SSL-Keystore neu erzeugen: Der Zugriff auf die Web-Oberfläche von SPONTS erfolgt verschlüsselt. Hierzu ist ein Schlüsselpaar notwendig, dass bei der Erstinstallation erzeugt werden muss. Geben Sie deshalb hier 'Yes' an und notieren Sie sich die beiden digitalen Fingerabdrücke der erzeugten Schlüssel - Sie benötigen Sie später, um beim Zugriff auf die Web-GUI zu prüfen, ob Sie mit der richtigen Maschine verbunden sind.
5. Start SPONTS at system boot?: SPONTS beim Booten automatisch starten? Auf SUSE- und Debian-Systemen kann SPONTS so eingerichtet werden, dass er beim Booten automatisch startet. Auf anderen Systemen konsultieren Sie bitte Ihre Systemdokumentation, wie dies einzurichten ist.
6. Start/Restart SPONTS now?: SPONTS jetzt starten? Ob der SPONTS jetzt sofort gestartet werden soll. Sie können dies auch händisch über `/etc/init.d/sponts start` erreichen.

3.5.2 Startmeldung prüfen

Nach dem Start des SPONTS können Sie mit dem Befehl

```
tail -f /var/log/sponts/sponts.log.0
```

die Startmeldungen verfolgen (Ende mit Strg-C). Sobald die Meldung

```
INFO: Starting Coyote HTTP/1.1 on http-25443
```

erscheint, können Sie auf die Web-GUI unter der URL

```
https://<SPONTS-Adresse>:25443/
```

zugreifen und sich mit dem Passwort start anmelden. Achten Sie hierbei auf die Angabe von https an Stelle von http, da es sich um eine verschlüsselte Verbindung handelt.

WICHTIG: Im Handbuch ist als Port 8443 angegeben. Da dieser Port auf Unix-Systemen oftmals von Tomcat-Installationen belegt ist, wird bei der Installation als Software-Paket der Port 25443 verwendet.

4 Einrichtung

Die IP-Adresseinstellungen müssen Sie an dem Gerät direkt vornehmen. Genauere Informationen hierzu finden Sie in der beiliegenden Kurzanleitung.

4.1 Einbindung ins Netzwerk

SPONTS ist ein SMTP-Proxy. Er sollte als alleiniger MX eingetragen sein, damit er von den Absendeservern direkt kontaktiert wird. Er leitet die Mail zum Backend weiter.

Um den maximalen Erfolg zu erreichen, sollte er der einzige MX sein, bzw. alle MX sollten SPONTS verwenden. In folgenden Konfigurationsbeispielen (Szenarien) wird davon ausgegangen, dass das Backend bereits an das Internet angeschlossen ist. Sie können für die Integration des SPONTS in Ihr Netzwerk eines der folgenden Szenarien auswählen:

4.1.1 Szenario 1: Backend hat eine öffentliche IP-Adresse

Das Backend hat eine aus dem Internet erreichbare IP-Adresse und nimmt auf dieser Mails entgegen. Um SPONTS einzubinden, bestehen zwei Möglichkeiten:

1. Die IP-Adresse des Backends wird geändert und SPONTS erhält die vorherige IP-Adresse.
2. SPONTS erhält eine andere ebenfalls aus dem Internet erreichbare IP-Adresse. Im DNS muss diese neue Adresse an Stelle der Adresse des Backends eingetragen werden.

DNS-Einträge haben eine gewisse „Lebenszeit“ von üblicherweise mehreren Stunden bis zu wenigen Tagen. So lange kann es dauern, bis alle Mailserver eine Änderung registriert haben und den gewünschten Server kontaktieren. Manche Mailserver ignorieren die angegebenen Lebenszeiten und arbeiten bis zu mehreren Wochen mit den veralteten Einträgen.

Welches dieser Verfahren Sie wählen, hängt vorrangig davon ab, ob sie die IP-Adresse ihres Backends ohne weiteres ändern können. Wenn ja, ist die erste Methode die bessere, da sie sofort aktiv wird. Das Backend kann nach der Umstellung auch im Intranet stehen, da es aus dem Internet nicht mehr direkt erreichbar sein muss.

Sollten Sie über eine vorgeschaltete Firewall verfügen, so können Sie auch SPONTS und das Backend im DNS eintragen und den SMTP-Zugriff auf das Backend in der Firewall sperren. Hierbei empfiehlt sich die Verwendung einer „REJECT“-Regel, die eine ICMP-Fehlermeldung zurück liefert, da sonst der Absendeserver jeweils bis zu 5 Minuten versucht, das Backend zu erreichen, bevor er aufgibt. Diese Konfiguration hat den Vorteil, dass sie durch einfaches Ändern der Firewall-Regeln die Mails wieder direkt über das Backend empfangen können.

4.1.2 Szenario 2: Bestehender MX wird über Port-Forwarding (Destination NAT) der Firewall angesprochen

Dieses Szenario ist einfacher als Szenario 1, da keine Änderungen an IP-Adressen und DNS-Einträgen notwendig sind. SPONTS muss eine eigene IP-Adresse erhalten und diese als Forward-Ziel in der Firewall eingetragen werden. Hierbei muss sichergestellt werden, dass bei eingehenden TCP-Verbindungen SPONTS die

original Absende-IP-Adresse des versendenden Mailservers und nicht diejenige der Firewall „sieht“. Bei aktuellen Firewalls ist dies die übliche Arbeitsweise und deshalb normalerweise kein Problem. Sie können dies leicht im SPONTS-Journal (vgl. 7.7 Journal, S. 77ff.) überprüfen: hier steht für jede empfangene oder abgewiesene Nachricht die IP-Adresse des Absendeservers drin. Diese darf für eine von außen empfangene Nachricht nicht die IP-Adresse der Firewall sein.

4.1.3 Szenario 3: Verteilte Standorte mit Port-Forwarding

Steht SPONTS nicht an dem Standort, an dem die Mailserver stehen, so muss der Datenverkehr entsprechend umgeleitet werden. Hierbei stellt sich das Problem, dass das Routing in beide Richtungen über den Port-Forwarder laufen muss, was beispielsweise mit IP-IP-Tunneln und Source-Based-Routing zu lösen ist.

Die Vorgehensweise ist folgende:

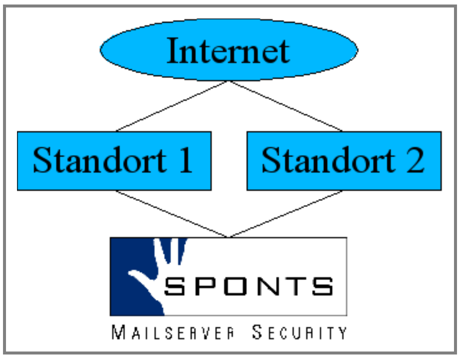


Abbildung 1 Mehrere Standorte mit einem zentralen SPONTS

- an den einzelnen Standorten wird jeweils ein GRE-Tunnel (**G**eneric **R**outing **E**ncapsulation) zum SPONTS aufgebaut
- ein Port-Forwarder leitet Anfragen über den Tunnel zum SPONTS weiter
- Antworten des SPONTS werden per Source-Based-Routing wieder über den Tunnel versendet
- mittels Masquerading (Source-NAT) wird die Adresse des SPONTS auf die des Port-Forwarders umgeschrieben

Als Beispiel folgt die Konfiguration unter Linux; sollten Sie ein anderes Betriebssystem für Ihren Port-Forwarder verwenden, so entnehmen Sie die entsprechenden Befehle dessen Handbuch. In dem Beispiel wird von folgender Konfiguration ausgegangen:

- Port-Forwarder am Standort 1 hat die IP-Adresse 192.168.1.1/24
- Port-Forwarder am Standort 2 hat die IP-Adresse 192.168.2.1/24
- SPONTS hat die IP-Adresse 192.168.3.1/24

Das Beispiel ist für zwei Standorte, ist aber auf beliebig viele Standorte erweiterbar.

Einrichtung des GRE-Tunnels

Ein GRE-Tunnel wirkt wie ein „virtuelles Netzwerkkabel“ zwischen zwei Rechnern mit jeweils entsprechenden virtuellen Schnittstellen. Dies hat den Vorteil, dass Routing-Einträge nur an den beiden Endpunkten erforderlich sind und nicht an allen Routern dazwischen. Eine Verschlüsselung oder Authentisierung des

Datenverkehrs erfolgt bei GRE-Tunneln nicht. Wie alle Schnittstellen erhält auch der Tunnel ein Netzwerk und eine IP-Adresse. In diesem Beispiel werden folgende Adressen verwendet:

- Tunnel Standort 1 (192.168.100.1) – SPONTS (192.168.100.2): 192.168.100.0/30
- Tunnel Standort 2 (192.168.100.5) – SPONTS (192.168.100.6): 192.168.100.4/30

Der SPONTS-Kernel hat Unterstützung für GRE-Tunnel integriert. Bei modularen Kerneln müssen Sie eventuell den Befehl

```
modprobe ip_gre
```

eingeben, um die Unterstützung zu laden. Um einen GRE-Tunnel aufzubauen, geben Sie folgenden Befehl ein:

```
ip tunnel add <name> mode gre remote <IP-Adresse Gegenseite> \
                              local <IP-Adresse lokal>
```

In diesem Beispiel wären folgende Befehle erforderlich:

Standort 1:

```
ip tunnel add sponts1 mode gre remote 192.168.3.1 local 192.168.1.1
ifconfig sponts1 192.168.100.1
route add -host 192.168.100.2 sponts1
```

Standort 2:

```
ip tunnel add sponts2 mode gre remote 192.168.3.1 local 192.168.2.1
ifconfig sponts2 192.168.100.5
route add -host 192.168.100.6 sponts2
```

SPONTS:

```
ip tunnel add sponts1 mode gre remote 192.168.1.1 local 192.168.3.1
ifconfig sponts1 192.168.100.2
route add -host 192.168.100.1 sponts1
ip tunnel add sponts2 mode gre remote 192.168.2.1 local 192.168.3.1
ifconfig sponts2 192.168.100.6
route add -host 192.168.100.5 sponts2
```

Danach muss die jeweilige Tunnel-Gegenseite mittels 'ping' erreichbar sein. Also beispielsweise auf dem SPONTS mit

```
ping 192.168.100.1
```

bzw.

```
ping 192.168.100.5
```

Die Befehle für den SPONTS müssen in die Datei '/system/etc/boot.local' eingetragen werden, damit sie nach einen Neustart automatisch ausgeführt werden.

Einrichtung des Port-Forwarders

Jetzt kann an den Standorten ein Port-Forwarder wie oben beschrieben eingerichtet werden. Als Ziel des Port-Forwarders muss jeweils die Tunnel-Adresse von SPONTS verwendet werden, also 192.168.100.2 für Standort 1 und 192.168.100.6 für Standort 2.

Auf dem SPONTS muss über den Menüpunkt '*SPONTS – Proxies*' (vgl. 7.3.9 Proxies, S. 61) für diese IP-Adressen ein entsprechender Proxy eingerichtet werden.

Rück-Routen mit Source-Based-Routing

Damit der Port-Forwarder korrekt arbeiten kann, müssen die Antworten von SPONTS an den richtigen Port-Forwarder zurückgesendet werden, d.h. Anfragen über Standort 1 müssen wieder zu Standort 1 gesendet werden und Anfragen von Standort 2 müssen zu Standort 2 geschickt werden. Hierzu unterstützt SPONTS Source-Based-Routing, d.h. zur Wahl einer Route wird nicht die Zieladresse, sondern die Quelladresse verwendet. Das Routing läuft hierbei in zwei Schritten ab:

1. Bestimmung einer alternativen Routing-Tabelle basierend auf der Absende-IP-Adresse
2. Bestimmung der Route basierend auf der Ziel-IP-Adresse aus der alternativen Tabelle.

Mehr Informationen hierzu finden Sie beispielsweise unter:
http://www.wlug.org.nz/SourceBasedRouting

Die entsprechenden Befehle mit Tabelle '100' für die Verbindung zu Standort 1 und Tabelle '101' für Standort 2 im Beispiel wären auf dem SPONTS:

```
ip rule add from 192.168.100.2 table 100
ip route add default via 192.168.100.1 table 100
ip rule add from 192.168.100.6 table 101
ip route add default via 192.168.100.5 table 101
```

Auch diese Befehle für den SPONTS müssen in die Datei '/system/etc/boot.local' eingetragen werden, damit sie nach einen Neustart automatisch ausgeführt werden.

4.2 Einstellen der IP-Konfiguration

Die Vorgehensweise zum Einstellen der IP-Konfiguration entnehmen Sie bitte der beiliegenden Kurzanleitung.

4.3 Verwendete TCP/UDP-Ports

SPONTS akzeptiert eingehende Verbindungen und baut Verbindungen nach außen auf. Die dafür standardmäßig verwendeten TCP-Ports sind:

Ziel-Port	Richtung	Funktion
22 TCP	eingehend	SSH/SFTP-Zugriff des Administrators
25 TCP	eingehend	SMTP-Eingang (einstellbar, Option '*SMTP-Portnummer des SPONTS*')
25 TCP	ausgehend	SMTP-Ausgang, Sender SMTP check
53 UDP	ausgehend	DNS Abfragen
80 TCP	ausgehend	automatische H+BEDV und Sophos Antivir-Updates
123 UDP	ausgehend	Zeitsynchronisation per NTP
3306 TCP	eingehend	MySQL-Zugriff
8443 TCP	eingehend	Web-GUI (einstellbar, Option '*HTTPS-Portnummer der Web GUI*')
11110 TCP	eingehend	UMS-POP3-Zugriff (einstellbar, Option '*POP3 Portnummer*')

Bei den Ports für SSH, MySQL und UMS-POP3 ist es nicht notwendig, dass diese aus dem Internet erreichbar sind. Sie sind nur für den Administrator vorgesehen und können mit einer Firewall gesperrt werden. Die verwendeten Ports der Web-GUI müssen nur dann vom Internet aus erreichbar sein, wenn Sie Zugriffe auf diese für Benutzer außerhalb Ihres Netzes erlauben wollen.

4.4 Zertifikate

SPONTS unterstützt verschlüsselte Verbindungen für alle Protokolle. Hierzu benötigt er ein SSL-Zertifikat, das während der Installation erzeugt wird. Dieses Zertifikat kann auch selbst erzeugt werden. Hierzu brauchen Sie das Programm „keytool“, das Bestandteil des „Java Runtime Environment (JRE)“ von Sun und auf dem SPONTS unter „/system/mount/java/bin/keytool“ verfügbar ist. Zum Erzeugen eines weiteren Zertifikates geben Sie folgenden Befehl ein:

```
keytool -genkey -keystore neuer.keystore \
       -keypass "geheim-key" -storepass "geheim-keystore" \
       -keyalg RSA \
       -dname "CN=ftpproxy.beispieldomain.net" \
       -alias sponts
       -validity 730
```

Das Zertifikat ist dann in der Datei 'neuer.keystore' unter dem Alias 'sponts' abgelegt und wird mit den Passwörtern 'geheim-keystore' für den Keystore und 'geheim-key' für den Key geschützt.

Wichtig: Damit SPONTS die Schlüssel entschlüsseln kann, muss als Keystore- und Schlüsselpasswort jeweils '......' (6 Punkte) eingegeben werden.

Dieses feste Passwort wurde gewählt, da der SPONTS das Passwort im Klartext kennen muss. Die Verwendung eines anderen Passwortes bietet deshalb keine zusätzliche Sicherheit.

Der Alias ist frei wählbar, muss aber für von SPONTS zu verwendende Schlüssel 'sponts' sein.

Hinweis: SPONTS vor der Version 2.2 hat als Alias noch 'jetty' verwendet, so dass Sie diesen Alias angeben müssen.

5 Zugriff auf die Web-Oberfläche (Web-GUI)

Die Web-Oberfläche ist standardmäßig erreichbar unter:
https://<ip-adresse>:8443/ (verschlüsselt)
Die Web-Oberfläche ist etwa 1-2 Minuten nach dem Starten von SPONTS verfügbar.

SPONTS wird über eine Web-Oberfläche konfiguriert. Hierbei kommt SSL-Verschlüsselung zum Einsatz. Eine Verbindung ohne SSL ist aus Sicherheitsgründen nicht möglich. Zudem müssen Sie in Ihrem Browser Cookies und JavaSkript aktivieren.

Für den SSL-verschlüsselten Zugang greifen Sie mit einem Browser per HTTPS auf Port 8443 der eingestellten IP-Adresse der SPONTS-Box zu. Ist die IP-Adresse beispielsweise 192.168.0.29, so greifen sie auf https://192.168.0.29:8443/ zu.

HTTPS-Verbindungen werden mit so genannten Zertifikaten autorisiert. SPONTS verwendet ein Zertifikat, das Ihr Browser nicht automatisch überprüfen kann und Sie deshalb davor warnt. Sie müssen daher das Zertifikat manuell überprüfen, um sicherzustellen, dass niemand Ihnen ein falsches Zertifikat unterschiebt und damit die Verbindung entschlüsseln kann. Hierzu müssen Sie sicherstellen, dass der „Fingerprint" des Zertifikats - eine Art Prüfsumme - mit demjenigen, der dem Gerät beiliegt, übereinstimmt. Es gibt zwei Prüfsummenarten:

- MD5
- SHA1

Nicht jeder Browser unterstützt beide Prüfsummenarten, es ist jedoch vollkommen ausreichend, nur eine davon zu überprüfen. Die genaue Vorgehensweise hierfür entnehmen Sie bitte der Anleitung Ihres Browsers. Exemplarisch werden hier die Meldungen des Microsoft Internet Explorers und des Mozilla Navigators gezeigt.

5.1 Microsoft Internet Explorer

Beim Zugriff auf die Seite erscheint zuerst folgende Meldung:

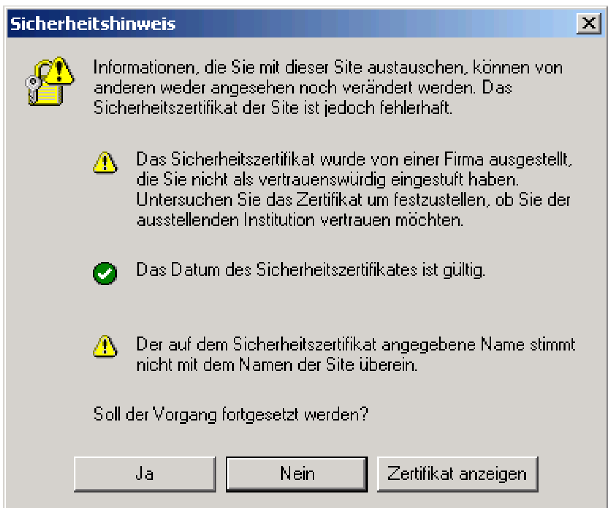


Abbildung 2: Sicherheitshinweis des IE

Die Meldung *„Der auf dem Sicherheitszertifikat angegebene Name stimmt nicht mit dem Namen der Site überein."* erscheint nur, wenn der in der SPONTS-IP-Konfiguration angegebene Hostname nicht mit dem Namen übereinstimmt, mit dem Sie auf SPONTS zugreifen.

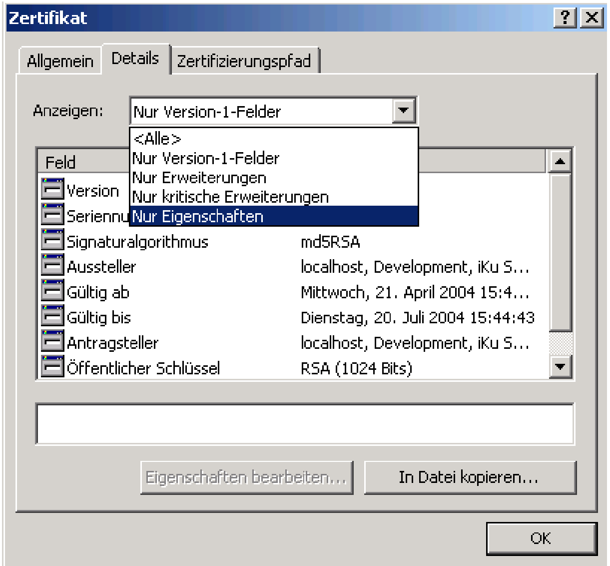


Abbildung 3: Zertifikat überprüfen (IE)

Klicken Sie jetzt auf *„Zertifikat anzeigen"*, um den folgenden Dialog zu erhalten und wählen Sie in diesem die Anzeige *„Nur Eigenschaften aus"*:

Es erscheint der folgende Dialog, der die SHA1-Prüfsumme des Zertifikates enthält:

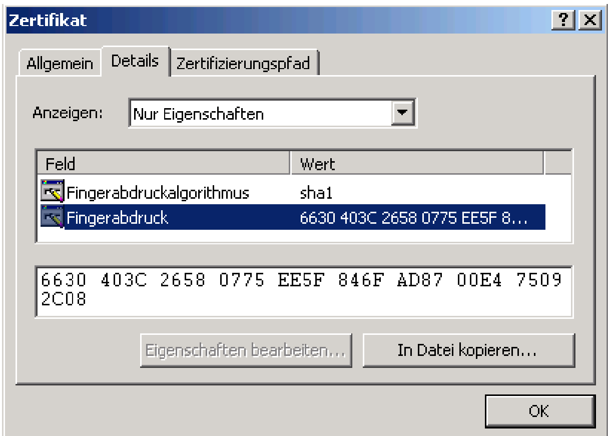


Abbildung 4: Überprüfung Fingerprint (IE)

Vergleichen Sie die angezeigte Prüfsumme mit der beiliegenden SHA1-Prüfsumme. Wenn Sie übereinstimmt, können Sie sicher sein, dass niemand die Verbindung abhören kann.

Sie können die Sicherheits-Dialoge erneut öffnen, indem Sie unten rechts auf das Symbol klicken.

5.2 Mozilla Navigator

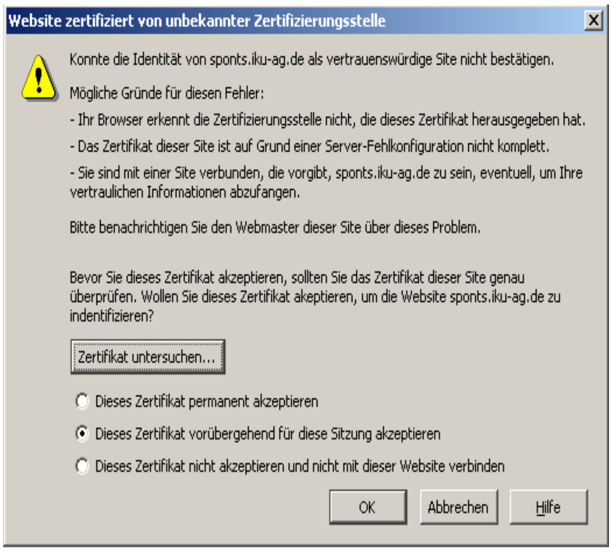


Abbildung 5: Überprüfung Zertifikat (Mozilla)

Beim Zugriff auf die Seite erscheint zuerst folgende Meldung:Falls vorher noch zusätzlich die Meldung *„Sicherheitsfehler: Domainnamen stimmen nicht überein"* erscheint, dann bedeutet das lediglich, dass der in der SPONTS-IP-Konfiguration angegebene Hostname nicht mit dem Namen übereinstimmt, mit dem Sie auf SPONTS zugreifen.

Klicken Sie jetzt auf *„Zertifikat untersuchen..."*, um den folgenden Dialog zu erhalten:

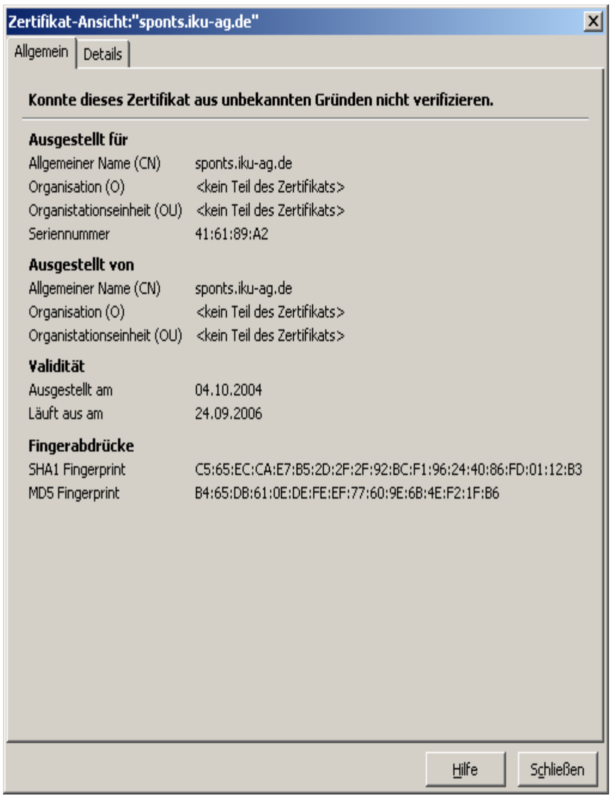


Abbildung 6 Überprüfung Fingerprint (Mozilla)

Unter dem Punkt *„Fingerabdrücke“* steht sowohl der SHA1-, als auch der MD5-Fingerprint. Vergleichen Sie die angezeigte Prüfsummen mit den beiliegenden Prüfsummen. Wenn Sie übereinstimmen, können Sie sicher sein, dass niemand die Verbindung abhören kann.

Sie können die Sicherheits-Dialoge erneut öffnen, indem Sie unten rechts auf das Symbol klicken.

5.3 Anmeldung an der WEB-GUI

Nachdem Sie sich mit Ihrem Browser mit dem SPONTS verbunden haben, stehen Ihnen zwei Möglichkeiten zur Verfügung, sich anzumelden:

- Benutzer-Anmeldung
- Administrator-Anmeldung (inkl. Domain-und Replay-Administratoren)



Abbildung 7 Anmeldung am SPONTS

Die *'Benutzer-Anmeldung'* ist für 'normale' Benutzer gedacht. Diese bekommen nach der Angabe ihrer E-Mail Adresse eine E-Mail mit Login-Link zugeschickt und können darüber ihre persönlichen Einstellungen vornehmen. (vgl. 6 Bedienung der Web-GUI für Benutzer, S. 18 ff.)

Über die *'Administrator-Anmeldung'* können sich alle Administoren (inkl. Domain- und Replay-Administratoren) anmelden. Um welche Administratoren-Rolle es sich handelt, wird automatisch ermittelt.

Der Administrator (Benutzername '*admin*') kann alle systemrelevanten Konfigurationen am SPONTS durchführen. (vgl. 7 Bedienung der Web-GUI für den Administrator, S. 33 ff.)

Domain-Administratoren sind nur in der ISP (Internet Service Provider) Version des SPONTS verfügbar. Hier kann ein vom Administrator festgelegter Donänen-Administrator die Einstellungen für eine einzelne Domäne ändern.

Replay-Administratoren können nur auf die Replay-Funktionen zugreifen (vgl. 7.8.3 Replay-Admins, S. 80).

6 Bedienung der Web-GUI für Benutzer

Geben Sie für die Anmeldung als Benutzer Ihre E-Mailadresse im Feld *'Benutzer-Anmeldung'* ein und klicken Sie auf den Button *'Zugangsberechtigung jetzt per E-Mail schicken'*.

Sie erhalten dann eine E-Mail mit einem Link zu Ihrer persönlichen Benutzerkonfiguration des SPONTS. Dieser Link ist standardmäßig für 8 Stunden gültig und verweist auf die Konfigurationsseite für den Benutzer. Bei einem grafischen E-Mail Programm (z.B. Mozilla Mail oder MS Outlook) müssen Sie nach dem Abrufen der Mail nur noch auf den Link in der Mail klicken. Alternativ können Sie den Login-Link auch aus der E-Mail kopieren und in der Adressleiste Ihrer Browsers einfügen. Sie werden dann auf die SPONTS Web-GUI weitergeleitet.

Die Oberfläche ist in vier Bereiche Unterteilt, welche in der folgenden Abbildung einzeln markiert sind:

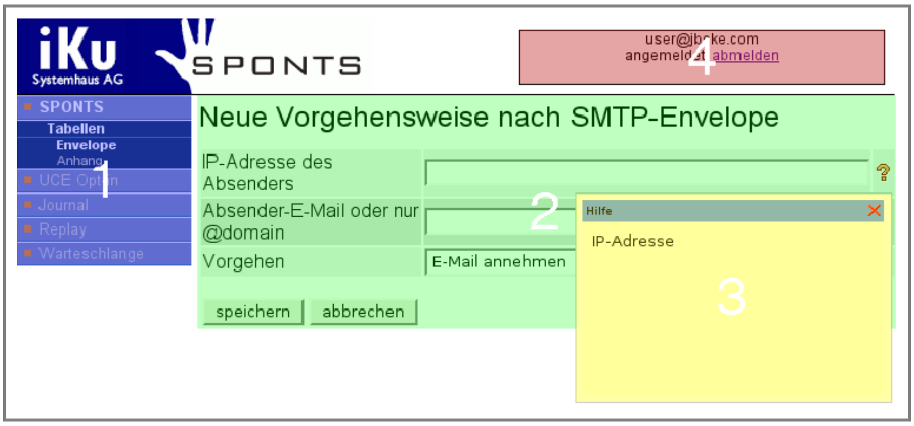


Abbildung 8 Bereiche der Web-GUI

1 Navigation

2 Datenbereich

3 Hilfebereich (erscheint nur, wenn Hilfe zu einem Element ausgewählt wurde)

4 Login-Informationen / Link zum Abmelden

6.1 Konfiguration des UCE-Moduls ('*SPONTS*')

UCE (Unsolicited Commercial E-Mail – Unerwünschte Werbemail) beinhaltet die Benutzereigenen Einstellungen zur Spam-Abwehr. Hier können Sie ein gesondertes Vorgehen anhand von Absenderadressen oder E-Mail Anhängen konfigurieren, bzw. Ihren UCE-Schutz für die im Login angegebene E-Mail Adresse aktivieren oder deaktivieren.

6.1.1 Kurzbeschreibung der Konfigurationsmöglichkeiten

Envelope – Vorgehen nach SMTP Envelope

Hiermit können Sie einzelne E-Mails mit bestimmten Eigenschaften (z.B. bestimmter Absender) z.B. in jedem Fall sperren (Blacklisting) oder in jedem Fall durchlassen (Whitelisting).

Anhang Filter

Hier können Sie bestimmte Anhänge anhand ihrer Dateiendung sperren oder erlauben.

UCE Opt-in – E-Mail Statistik und Spam Blockierung aktivieren / deaktivieren

Einstellungen zum Spam-Schutz allgemein

6.1.2 Envelope – Vorgehen nach SMTP Envelope

Black-/Whitelisten von Absende IP-Adressen, -E-Mails und -Domains

Menüpunkt: *'SPONTS → Tabellen → Envelope'*

Klicken Sie im Navigationsbereich auf *'SPONTS → Tabellen → Envelope',* um Ihre Black/Whitelisten zu bearbeiten.

Whitelist: Sie erlauben den Empfang von E-Mails von der IP-Adresse, Domain oder E-Mailadresse, die Sie auf die Whitelist setzen.
Blacklist: Sie verbieten den Empfang von E-Mails von der IP-Adresse, Domain oder E-Mailadresse, die Sie auf die Blacklist setzen.

Neuen Eintrag in der Black-/Whitelist erzeugen

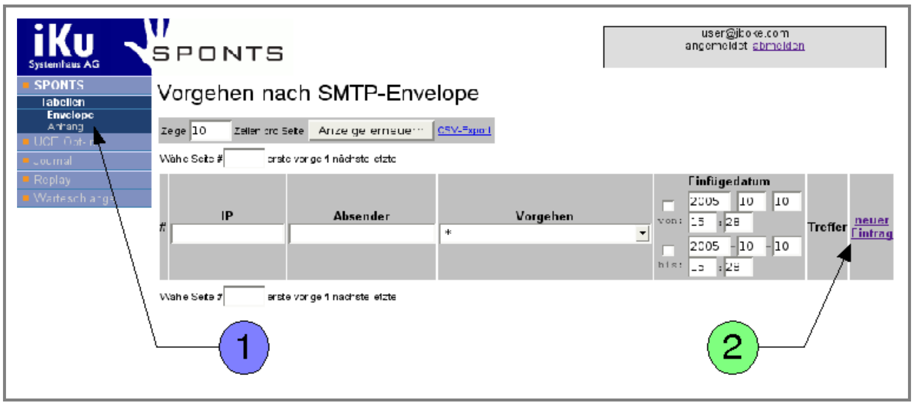


Abbildung 10 Eintrag in Black-/Whitelisten

- Wählen Sie in der Navigation den Punkt ①: *'SPONTS → Tabellen → Envelope'*
- Klicken dann auf ② *'neuer Eintrag'*, um einen neuen Eintrag anzulegen:



Abbildung 11: Eintrag in Black/Whitelist bearbeiten

- Geben Sie dann die *'IP-Adresse des Absenders'* , die Sie auf die Blacklist/Whitelist setzen möchten, ein.
- Geben Sie die E-Mailadresse oder Domain (*'Absender E-Mail oder nur @Domain'*), die Sie auf die Blacklist /Whitelist setzen möchten, ein.
- Wählen Sie in der Box (*'Vorgehen'*), was mit einer E-Mail, welche an Sie gerichtet ist, geschehen soll. Dabei stehen Ihnen die folgenden Vorgehensweisen zur Verfügung:
  - *'E-Mail zurückweisen'* oder auf die
    Dies entspricht einem sogenannten **Blacklisting**. Eingehende E-Mails, welche auf die Einstellungen zutreffen werden immer abgelehnt.
  - *'E-Mail* annehmen'
    Eingehende E-Mails, welche auf die Einstellungen zutreffen werden angenommen. Es werden jedoch weiterhin Virenprüfungen an der eingehenden E-Mail vorgenommen, was je nach Konfiguration durch Ihren Administrator zu einer Ablehnung wegen Virenverseuchung führen. Diese Einstellung entspricht einem sogenannten **Whitelisting**.
  - *'E-Mail niemals zurückweisen'*
    Durch diese Einstellung können Sie verhindern, dass E-Mails, welche als UCE oder Virenverseucht erkannt werden, abgewiesen werden. Es wird lediglich eine Warnung in den Mailbetreff eingetragen, falls dies vom Administrator konfiguriert wurde.
  - *'immer annehmen, nicht auf Viren* prüfen'
    Eingehende E-Mails, welche auf diese Einstellungen zutreffen, werden weder auf UCE, noch auf Viren geprüft.
  - *'erlaube verschlüsselte Dateien'*
    Eingehende E-Mails, welche aufgrund von verschlüsselten Dateien nicht auf Viren gescannt werden können, werden durch diese Einstellung dennoch angenommen. Andernfalls kann es je nach Konfiguration durch Ihren Administrator vorkommen, dass solche Dateien abgelehnt werden, da ihre Inhalte nicht überprüft werden können.
  - *'Postfach ist eine Spamfalle'*
    Absendeserver von E-Mails, welche auf diese Einstellungen zutreffen, werden in ihrem Sendeversuch für eine bestimmte Zeit blockiert, bevor die E-Mail aufgrund von UCE abgelehnt wird. Eine Spamfalle bezeichnet solche Postfächer, welche zur Senkung der Sendeleistung von Spammern genutzt werden kann.
- Klicken Sie auf *'speichern'*, um Ihren Eintrag abzuspeichern.
- Mit einem Klick auf ? sehen Sie im Hilfebereich den entsprechenden Hilfetext. Der Hilfetext bleibt so lange stehen, bis Sie einen neuen Hilfetext auswählen, oder diesen mit einem Klick auf ✕ im Hilfebereich schließen.

Die Eintragungen, die Sie an dieser Stelle machen, können zu einem sehr frühen Zeitpunkt der E-Mailübertragung geprüft werden und wirken so vor später folgenden Überprüfungen. Sollte Ihr Administrator jedoch ebenfalls Einstellungen an diesen Tabellen vorgenommen haben, so überschreiben die systemweiten Einstellungen Ihre persönlichen Einstellungen.

Beispiele

Alle Nachrichten eines Absenders (z.B. 'newsletter@jboke.de') durchlassen

IP-Adresse des Absenders	leer
Absender E-Mail oder @domain	'newsletter@jboke.de'
Vorgehen	*'E-Mail annehmen'*

Absende-Domain komplett freischalten (z.B. 'jboke.de')

IP-Adresse des Absenders	leer
Absender E-Mail oder @domain	'@jboke.de'
Vorgehen	*'E-Mail annehmen'*

Spam-Server sperren

IP-Adresse des Absenders	eintragen
Absender E-Mail oder @domain	leer
Vorgehen	*'E-Mail zurückweisen'*

Absender sperren (z.B. 'stoerenfried@jboke.de')

IP-Adresse des Absenders	leer
Absender E-Mail oder @domain	'stoerenfried@jboke.de'
Vorgehen	*'E-Mail zurückweisen*

Einträge in der Black-/Whitelist bearbeiten/löschen

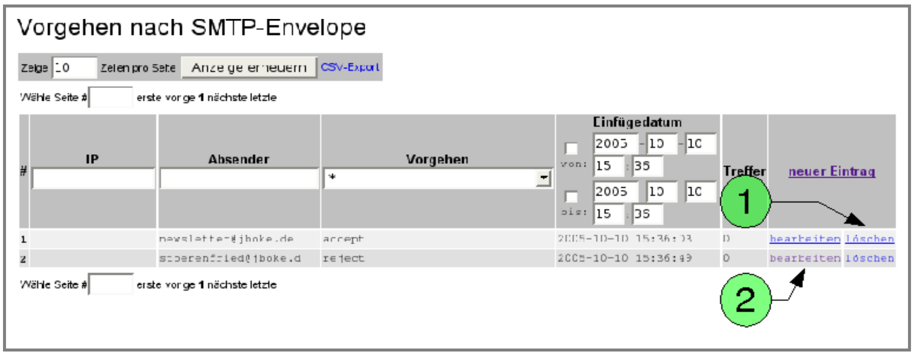


Abbildung 12: Black/Whitelisten bearbeiten

- Um einen Eintrag zu löschen klicken Sie in der entsprechenden Zeile auf ① *'löschen'*.
- Um einen Eintrag zu bearbeiten klicken Sie in der entsprechenden Zeile auf ② *'bearbeiten'*.
  Ändern Sie die Eingaben (vgl. 6.1.2 Neuen Eintrag in der Black-/Whitelist erzeugen, S. 19) und klicken Sie *'speichern'* zum Abspeichern oder klicken Sie *'abbrechen'* um Ihre Änderungen zu verwerfen.

Envelope-Black-/Whitelist nach Einträgen durchsuchen

Da die Black-/Whitelisten durchaus sehr groß werden können, haben Sie die Möglichkeit, nach einzelnen Einträgen zu suchen. Dabei können Sie nach verschiedenen Kriterien suchen, müssen aber nicht alle angeben. Lassen Sie bei

der Suche eines der Felder leer, so werden *alle* Ergebnisse für dieses Feld angezeigt.

Grundsätzlich haben Sie folgende Suchoptionen:

- Geben Sie im Eingabefeld *'IP'* die IP-Adresse, nach welcher Sie in Ihrer Black-/ Whitelist suchen, ein.
- Geben Sie im Eingabefeld *'Absender'* die E-Mailadresse oder Domain an, nach der Sie in Ihrer Black-/Whitelist suchen.
- Wählen in der *'Vorgehen'* Box aus, ob Sie nach allen Einträgen (*'*'*), nach Einträgen in der Blacklist (*'zurückweisen'*) oder nach Einträgen in der Whitelist (*'annehmen'*) suchen.
- Nutzen Sie die Eingabefelder *'Einfügedatum'*, um nach Einträgen in der Black-/Whitelist zu einem bestimmten Zeitpunkt oder innerhalb eines bestimmten Zeitraums zu suchen.

Ansicht aktualisieren

Klicken Sie *'Anzeige erneuern'*, um die Ansicht zu aktualisieren.

Angezeigte Zeilenanzahl pro Seite wählen

Geben Sie die Anzahl der Zeilen an, die pro Seite angezeigt werden sollen.

Angezeigte Seite Wählen

Geben Sie die Seitenzahl der Seite mit Einträgen ein, die angezeigt werden soll.

Exportieren und speichern der Black/Whitelist

Klicken Sie auf *'CSV-Export'*, um die vollständige Liste zu speichern. Die Speicherung der Liste erfolgt unabhängig von einer möglichen Filterung der Listeneinträge. Diese Liste kann in Tabellenkalkulationsprogrammen geöffnet werden, als Trennzeichen der Spalten wird ein Semikolon ';' verwendet.

6.1.3 Anhang Filter

Menüpunkt: *'SPONTS → Tabellen → Anhang'*

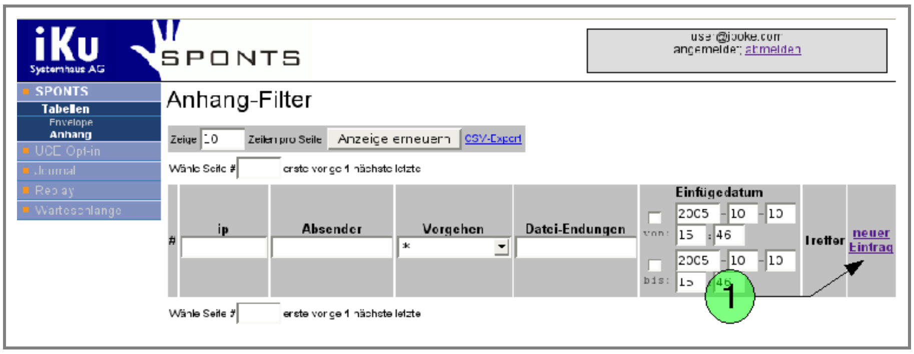


Abbildung 13Anhang-Filter

Anhänge in E-Mails werden oft zum Transport von Malware (z.B. Viren oder Trojaner) genutzt. Bestimmte Anhänge (z.B. ausführbare Dateien) stellen daher oft ein hohes Sicherheitsrisiko dar. Sie können hier grundsätzlich bestimmte Dateien sperren, um dieses Risiko zu minimieren. Dabei werden die Dateien (genau wie von

Windows) an der Dateiendung identifiziert. SPONTS kann alle Anhänge anhand der Dateiendung durchlassen oder entfernen. Wird ein Anhang von einer E-Mail entfernt, so bleibt die E-Mail ansonsten unverändert. Lediglich der Anhang wird durch einen Hinweis ersetzt, der den Dateinamen des Anhangs enthält und eine Identifikationsnummer (ID), über die Sie bei Ihrem Mailadministrator den Anhang anfordern können.

Beispiel für eine E-Mail mit entferntem Anhang

```
Hallo Hans,
anbei ein toller Bildschirmschoner
Gruß,
Frank
_____________________________________________

The file 'Bildschirmschoner.exe' has been removed by SPONTS
Journal entry for this mail:
https://sponts/journal/Details.jsp?id=100AF3C8BF4-0
```

Der Hinweis auf den entfernten Anhang befindet sich unterhalb des Textes der E-Mail. Sie können diesem Hinweis den Dateinamen und die ID entnehmen. Falls Ihr SPONTS über das Modul *'Journal'* verfügt, können Sie über den Link weitere Informationen zu dieser E-Mail und des(der) Anhänge bekommen.

Beachten Sie, dass Sie entweder einzelne Anhänge freischalten (*'annehmen'*) *oder* entfernen (*'zurückweisen'*). Erzeugen Sie Einträge mit der Regel *'annehmen'*, werden alle anderen Anhänge entfernt. Sollten Sie Einträge mit der Regel *'ablehnen'* erzeugen, werden alle anderen Anhänge durchgelassen.

Der Administrator des SPONTS hat die Möglichkeit, globale Listen zu erstellen, die den Benutzerlisten vorgeschaltet sind. Daher kann es vorkommen, dass Sie bestimmte Anhänge freigeschaltet haben, Sie diese aber trotzdem nicht empfangen können. Fragen Sie im Zweifelsfall Ihren Administrator.

Neuer Eintrag in die Anhangfilter-Liste

Mit einem Klick auf ① *'neuer Eintrag'* werden Sie zum Eingabedialog weitergeleitet:

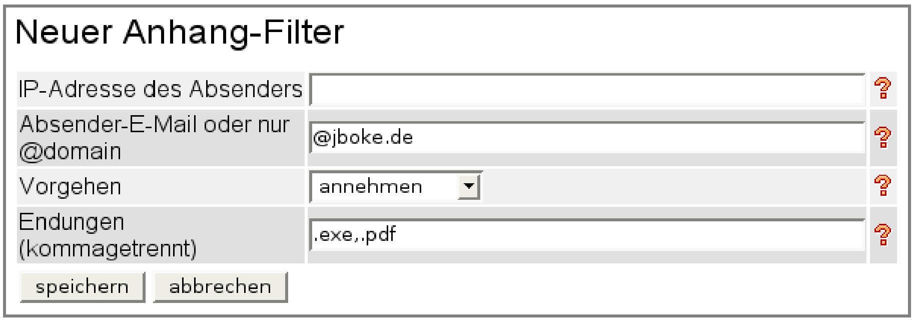


Abbildung 14: Anhangfilter einfügen

- Geben Sie die *'IP-Adresse des Absenders'*, von welchem Sie eingehende E-Mails mit Dateianhängen erlauben oder verbieten möchten, ein. Diese Funktion wird allerdings nur in Sonderfällen benötigt. Normalerweise können Sie dieses Feld leer lassen.

- Geben Sie die E-Mailadresse oder Absende-Domain (*'Absender E-Mail oder nur @domain'*), für welche Sie eingehende E-Mails mit Dateianhängen erlauben oder verbieten möchten, ein.
- Wählen Sie bei *'Vorgehen'*, ob Sie E-Mails mit Anhängen für die eingegebene IP-, E-Mail-Adresse oder Domain erlauben (*'annehmen'*) oder verbieten (*'zurückweisen'*) möchten.
- Geben Sie die Dateiendung des Anhangs (*'Endungen (kommagetrennt)'*), für welches Sie den Empfang erlauben oder verbieten, ein. Geben Sie mehrere Endungen von Dateianhängen an, so müssen diese durch Kommata getrennt werden (Bsp.: '.exe,.bat'). Sie sollten an dieser Stelle auch den Punkt (.) vor der Dateiendung angeben, da sonst auch ungewollt andere Anhänge entfernt werden könnten. Wenn Sie beispielsweise die Dateiendung „ml" eintragen, sind hier auch Anhänge mit der Endung „.html" betroffen.
- Klicken Sie auf *'speichern'*, um Ihren Eintrag abzuspeichern.
- Mit einem Klick auf ? sehen Sie den Hilfetext. Der Hilfetext bleibt so lange stehen, bis Sie einen neuen Hilfetext auswählen, oder diesen mit einem Klick auf ✕ im Hilfebereich schließen.

Beispiele

Nur Nachrichten mit .doc-Anhängen eines Absenders durchlassen

IP-Adresse des Absenders	leer
Absender E-Mail oder @domain	eintragen
Vorgehen	*'annehmen'*
Erweiterungen	'.doc'

Nur .pdf-Anhänge einer Absende-Domain komplett freischalten

IP-Adresse des Absenders	leer
Absender E-Mail oder @domain	@domainname
Vorgehen	*'annehmen'*
Erweiterungen	'.pdf'

Mails mit .bat- und .exe-Dateianhängen von einem Server sperren

IP-Adresse des Absenders	eintragen
Absender E-Mail oder @domain	leer
Vorgehen	*'ablehnen'*
Erweiterungen	'.bat,.exe'

Absender mit .pif-Dateianhängen sperren

IP-Adresse des Absenders	leer
Absender E-Mail oder @domain	eintragen
Vorgehen	*'ablehnen'*
Erweiterungen	'.pif'

Einträge in der Anhangfilter-Liste bearbeiten/löschen

Sie haben hier – ähnlich wie beim Bearbeiten der Black/Whitelisten – die Möglichkeit, nach einzelnen Einträgen zu suchen. Dabei können Sie sich nach verschiedenen Kriterien suchen, müssen aber nicht alle angeben. Lassen Sie bei der Suche eines der Felder leer, so werden *alle* Ergebnisse für dieses Feld angezeigt.

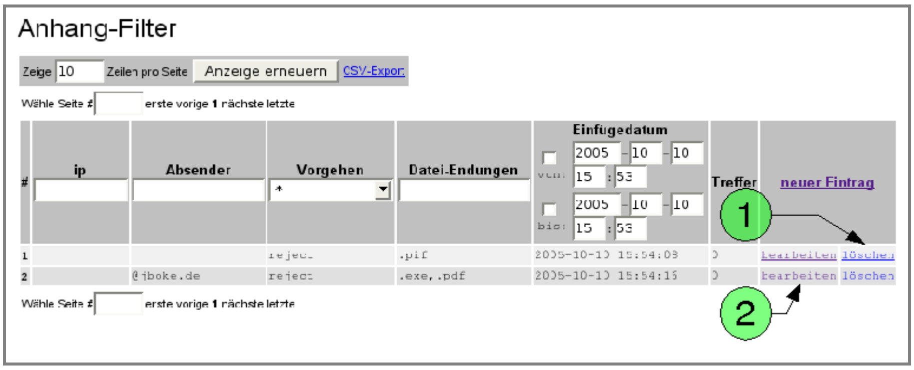


Abbildung 15: Anhang-Filter bearbeiten/löschen

- Um einen Eintrag zu löschen, klicken Sie in der entsprechenden Zeile auf ① '*löschen*'.
- Um einen Eintrag zu bearbeiten, klicken Sie in der entsprechenden Zeile auf ② *'bearbeiten'*.
- Ändern Sie die Eingaben (vgl. 6.1.3 Neuer Eintrag in die Anhangfilter-Liste, S. 23) und klicken Sie *'speichern'* zum Abspeichern oder klicken Sie auf *'abbrechen'*, um Ihre Änderungen zu verwerfen.

Anhangfilter-Liste nach Einträgen durchsuchen

- Geben Sie im Eingabefeld *'IP'* die IP-Adresse, nach welcher Sie in Ihrer Anhangfilter-Liste suchen, ein.
- Geben Sie im Eingabefeld *'Absender'* die E-Mailadresse oder Domain an, nach der Sie in Ihrer Black-/Whitelist suchen.
- Wählen in der Box *'Vorgehen'* aus, ob Sie nach allen Einträgen (*'*'*), nach Einträgen in der Blacklist (*'ablehnen'*) oder nach Einträgen in der Whitelist (*'annehmen'*) suchen.
- Geben Sie im Eingabefeld *'Datei-Endungen'* die Endung der Dateianhänge, nach denen Sie suchen, ein. An dieser Stelle können Sie jedoch nur eine
- Nutzen Sie die Eingabefelder *'Einfügedatum'*, um nach Einträgen in der Black-/ Whitelist zu einem bestimmten Zeitpunkt oder innerhalb eines bestimmten Zeitraums zu suchen.

Ansicht aktualisieren

Klicken Sie *'Ansicht erneuern'*, um die Ansicht zu aktualisieren.

Angezeigte Zeilenanzahl pro Seite wählen

Geben Sie hier die Anzahl der Zeilen an, die pro Seite angezeigt werden sollen.

Angezeigte Seite Wählen

Geben Sie die Seitenzahl der Seite mit Einträgen ein, die angezeigt werden soll.

Exportieren und speichern der Anhangfilter-Liste

Klicken Sie auf *'CSV-Export'*, um die Liste zu speichern. Diese Liste kann in Tabellenkalkulationsprogrammen geöffnet werden. Als Trennzeichen der Spalten wird ein Semikolon ';' verwendet.

6.1.4 UCE Opt-in

Menüpunkt: *'UCE Opt-in'*



Abbildung 16: UCE Einwilligung

Spamabwehr aktivieren

Um das Blocken von UCE zu aktivieren, setzen Sie das Häkchen bei *'Spamabwehr aktivieren'*. Sollten Sie das Blocken von eingehenden Spam-Mails nicht aktivieren, so werden diese nur als UCE markiert und durchgelassen.

Klicken Sie auf *'speichern'*, um Ihre Änderungen zu speichern.

Die Einwilligung zur Spamabwehr ist nötig, da dies einer Nachrichtenunterdrückung (Zensur) Ihres E-Mailverkehrs entspricht und aufgrund des Fernmeldegesetzes nur in Verbindung mit Beriebsvereinbarungen o.ä. von Ihrem Administrator global eingerichtet werden darf.

Mail-Statistik aktivieren

Um eine Statistik Ihrer eingehenden Mails zu erhalten, setzen Sie das Häkchen bei 'E-Mail-Statistik aktivieren'. Sie erhalten dann täglich per E-Mail eine Statistik über Ihre eingehenden E-Mails.

Klicken Sie auf *'speichern'*, um Ihre Änderungen zu speichern.

Beispiel: Mailstatistik

```
*** SPONTS daily mail report for user@jboke.com ***

Report for Tue, 2 Nov 2004
delivered: 7
queued:    0
aborted:   6
blocked:   6
              Mails with status aborted:
Received From                           Subject
-------- ------------------------------ -----------------------
02:14:50 <davis@dyn-28.direct.ca>
04:53:25 <5Ysuzanne44@LyBp73fXmv.net>
11:49:32 <michael.greenepc@archeveche-m
13:35:16 <lloydkochhn@archeveche-mtl.qc
13:35:41 <shelbynicholson_no@bio.mach.m
19:12:04 <natalia@nikhefk.nikhef.nl>

            Mails with status blocked:
Received From                           Subject
-------- ------------------------------ -----------------------
10:31:06 <bobbicash_gx@blues.uab.es>
05:34:11 <cruzbutts_fs@asbjerg.dk>
08:41:41 <vshowroom@linedmainly.com>
08:42:39 <vshowroom@ardiscantwin.com>
11:40:46 <10129.10616841@ozalya.com>    Wanted: Real Estate Investor
15:53:57 <edbahirfasheyiky_004@virgilio PARTERNSHIP REQUIRED!!!
```

6.1.5 Einweg-/Wegwerfadressen

Unter Einweg- bzw. Wegwerfadressen verstehen sich E-Mail Adressen zur kurzzeitigen Nutzung. Diese können z.B zur Anmeldung auf Webseiten genutzt werden, wobei eine Einwegadresse im Format

`[schlüsselwort].[anzahl].[empfänger]`

oder

`[schlüsselwort].[empfänger]` angegeben werden kann.

Benutzer, die sich zur Nutzung der Einwegadressen angemeldet haben, müssen die selbst erzeugten Adressen nicht im SPONTS angeben. Eine neue Einwegadresse wird vom System übernommen und die mit dieser Adresse angegebene Anzahl von E-Mails wird an den eigentlichen Empfänger weitergeleitet.

Beispiel:
einwegadresse.12.benuter@domain.de

E-Mails an diese Adresse werden an den Empfänger <benutzer@domain.de> weitergeleitet. Nach 12 empfangenen E-Mails wird diese Adresse blockiert.

Die Anzahl der über eine Einwegadresse empfangenen E-Mails, sowie die noch verfügbare Anzahl von E-Mails, bevor der Empfang blockiert wird, ist über die Liste der Adressen und Empfänger einsehbar und konfigurierbar.

Einwilligung

Menüpunkt: '*UCE Opt-in → Einwegadressen*'

Um Einwegadressen für Ihre Mailadresse nutzen zu könne, müssen Sie die Einwilligung für diese aktivieren. Klicken Sie auf '*speichern*', um Ihre Einstellung im System zu speichern.



Abbildung 17 Einwilligung zu Einwegadressen

Bearbeiten von Einwegadressen

Menüpunkt: *'UCE Opt-in → Einwegadressen → Adressen und Empfänger'*

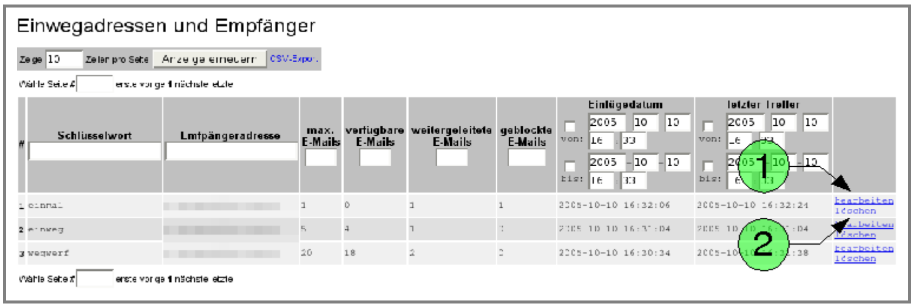


Abbildung 18 Einwegadressen bearbeiten

Nachdem Sie eine Einwilligung zur Nutzung von Einwegadressen abgegeben haben, können Sie diese nutzen. Die von Ihnen in Verwendung befindlichen Einwegadressen können Sie über den Menüpunkt '*Adressen und Empfänger*' einsehen und teilweise bearbeiten. Auf dieser Übersichtsseite sehen Sie zu jeder Einwegadresse das verwendete Schlüsselwort, Ihre eigentliche Empfängeradresse, sowie einige Zahlen zur betreffenden Adresse:

- **max. E-Mails**
  Maximalzahl der E-Mails, welche über diese Einwegadresse empfangen werden kann. Diese Anzahl haben Sie mit der Eingabe der Einwegadresse auf einer Internetseite mit der Anzahl zwischen Schlüsselwort und Ihrer Adresse angegeben. Haben Sie dort keine Anzahl angegeben, so wird die Maximalzahl auf einen durch den Administrator festgelegten Einstellung festgesetzt. Diese Maximalzahl einer Einwegadresse können Sie über ① '*bearbeiten*' verändern, jedoch nie höher, als die durch den Administrator festgelegte Zahl setzen.
- **verfügbare E-Mails**
  Anzahl der noch über diese Einwegadresse empfangbaren E-Mails. Sobald die Anzahl der verfügbaren E-Mails auf 0 gesunken ist, werden E-Mails an diese Adresse abgelehnt. Sie können die Anzahl der verfügbaren E-Mails über ① '*bearbeiten*' verändern, jedoch nie höher, als die durch den Administrator festgelegte Zahl setzen.
- **weitergeleitete E-Mails**
  Hier sehen Sie, wie viele E-Mails bisher über diese Einwegadresse an Ihre eigentliche E-Mailadresse weitergeleitet wurden. Diese Zahl kann von Ihnen nicht verändert werden.

- **geblockte E-Mails**
  Hier sehen Sie, wie viele E-Mails an diese Einwegadresse bisher geblockt wurden. Diese Zahl kann von Ihnen nicht verändert werden.

Um eine Einwegadresse zu bearbeiten, klicken Sie auf ① 'bearbeiten'. Sie werden dann auf eine entsprechende Seite zur Bearbeitung der Einwegadresse weitergeleitet.
Um eine Einwegadresse zu löschen, klicken Sie auf 'löschen'. Auf einer Bestätigungsseite werden Sie danach gefragt, ob Sie die entsprechende Einwegadresse wirklich löschen wollen.

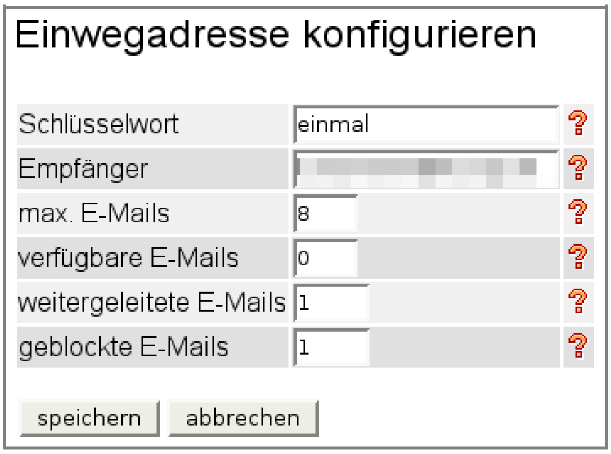


Abbildung 19Einwegadresse bearbeiten

Auf der Konfigurationsseite einer Einwegadresse sehen Sie ebenfalls alle Daten zu dieser Adresse. Sie dürfen die Maximalzahl der E-Mails und die Anzahl der verfügbaren E-Mails verändern und können so kontrollieren, ob sie mehr oder weniger E-Mails über eine Einwegadresse empfangen möchten.
Im Allgemeinen empfiehlt es sich, die Zahl der verfügbaren E-Mails wieder zu erhöhen, falls diese auf 0 zurückgegangen ist, Sie aber noch mehr Mails über diese Adresse empfangen möchten.
Nachdem Sie Änderungen an einer Einwegadresse vorgenommen haben, klicken Sie auf '*speichern*', um diese im System zu speichern. Klicken sie auf '*abbrechen*', um Ihre Änderungen zu verwerfen.

6.2 Journal verwenden

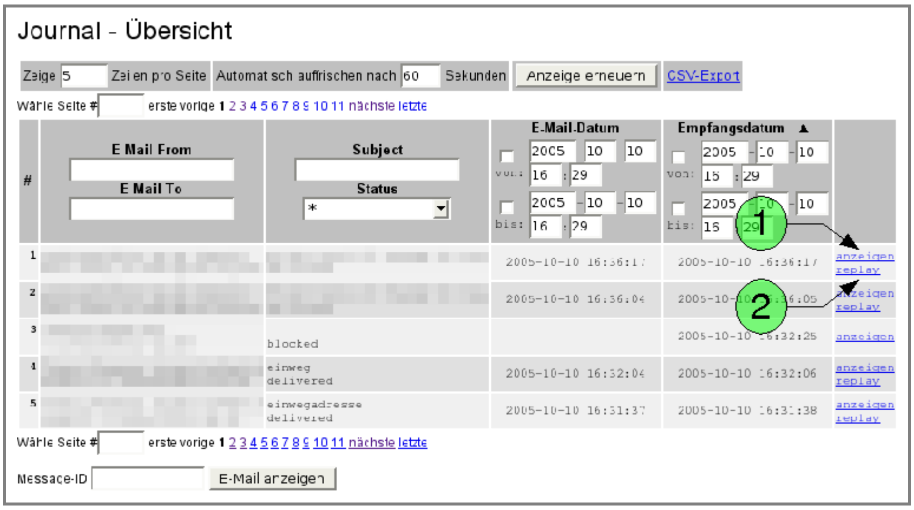


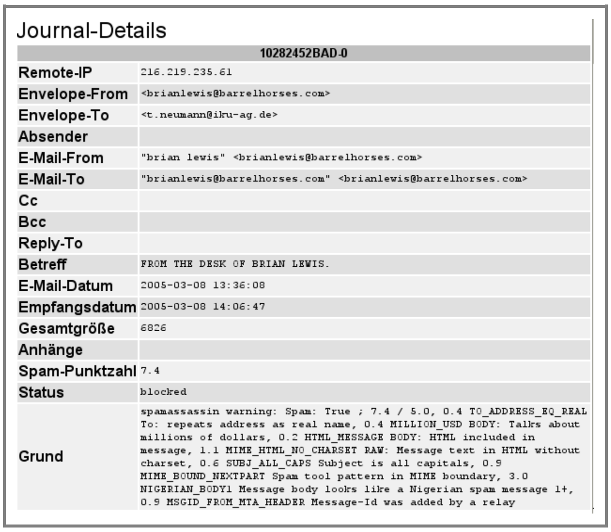
Abbildung 20: Journal-Übersicht

Sie haben hier – ähnlich wie beim Bearbeiten der Black/Whitelisten - die Möglichkeit, nach einzelnen Einträgen zu suchen. Dabei können Sie nach verschiedenen Kriterien suchen, müssen aber nicht alle angeben. Lassen Sie bei der Suche eines der Felder leer, so werden *alle* Ergebnisse für dieses Feld angezeigt.

Das Journal enthält einen Eintrag für jede eingegangene, abgewiesene und versendete Mail. Die Spalte *'Status'* enthält Informationen über den Zustand einer Mail und kann einen der folgenden Werte annehmen:

- *'aborted'*
  Der Versender hat die Verbindung getrennt, bevor die Nachricht vollständig übermittelt wurde.
- *'blocked'*
  Die eingegangene E-Mail wurde blockiert. Gründe für das Blockieren der E-Mail können über die Details der E-Mail eingesehen werden und sind unter dem Punkt 'Reason' vermerkt.
- *'queued'*
  Die Nachricht wurde in die Warteschlange eingestellt und wartet auf Zustellung zum entsprechenden Backend oder E-Mail Server.
- *'delivered'*
  Die Nachricht wurde erfolgreich an das Backend oder den E-Mail Server ausgeliefert.
- *'exception'*
  Bei der Verarbeitung ist in SPONTS ein nicht abgefangener Fehler auftreten. Gründe dieses Fehlers können über die Details der E-Mail eingesehen werden und sind unter dem Punkt 'Reason' vermerkt.

Klicken Sie bei der entsprechenden E-Mail auf den Link ① *'anzeigen'*, so erhalten Sie detaillierte Informationen zu dieser Mail:



Journal-Details

10282452BAD-0	
Remote-IP	216.219.235.61
Envelope-From	<brianlewis@barrelhorses.com>
Envelope-To	<t.neumann@iku-ag.de>
Absender	
E-Mail-From	"brian lewis" <brianlewis@barrelhorses.com>
E-Mail-To	"brianlewis@barrelhorses.com" <brianlewis@barrelhorses.com>
Cc	
Bcc	
Reply-To	
Betreff	FROM THE DESK OF BRIAN LEWIS.
E-Mail-Datum	2005-03-08 13:36:08
Empfangsdatum	2005-03-08 14:06:47
Gesamtgröße	6826
Anhänge	
Spam-Punktzahl	7.4
Status	blocked
Grund	spamassassin warning: Spam: True ; 7.4 / 5.0, 0.4 TO_ADDRESS_EQ_REAL To: repeats address as real name, 0.4 MILLION_USD BODY: Talks about millions of dollars, 0.2 HTML_MESSAGE BODY: HTML included in message, 1.1 MIME_HTML_NO_CHARSET RAW: Message text in HTML without charset, 0.6 SUBJ_ALL_CAPS Subject is all capitals, 0.9 MIME_BOUND_NEXTPART Spam tool pattern in MIME boundary, 3.0 NIGERIAN_BODY1 Message body looks like a Nigerian spam message 1+, 0.9 MSGID_FROM_MTA_HEADER Message-Id was added by a relay

Abbildung 21: Journal-Details

6.2.1 Verbindungs- und Nachrichten-ID

Die eindeutige Verbindungs-ID, welche als Kopfzeile in den Journal-Details angezeigt wird, besteht aus Hexadezimal-Zeichen, beispielsweise '10282452BAD-0'. Üblicherweise wird pro Verbindung nur jeweils eine Nachricht übertragen, aber insbesondere bei Mailinglisten können es auch mehrere sein. Jede Nachricht wird von 0 beginnend durchnummeriert, d.h. '10282452BAD-0' ist die erste Nachricht, die in der Verbindung '10282452BAD' übermittelt wurde. Diese IDs finden Sie auch in den Logdateien.

6.3 Replay verwenden

Geht eine einzelne Mail verloren - beispielsweise durch Viren oder Fehlbedienung - so kann sie über die Replay-Funktion beliebig oft erneut versendet werden. Hierzu wählt man in der Web-GUI den Punkt *'Replay'* an.

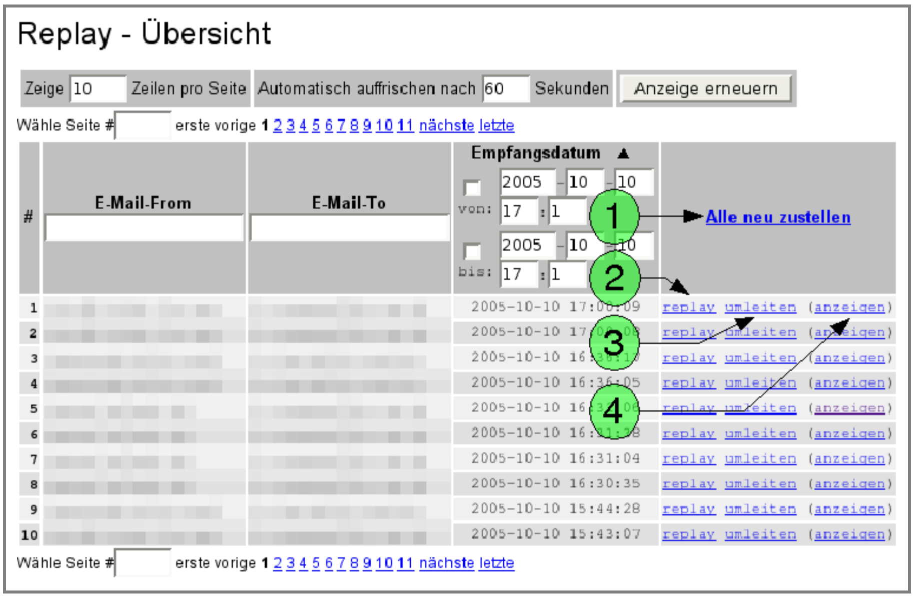


Abbildung 22: Auszug Replay

Sie haben hier – ähnlich wie beim Bearbeiten der Black/Whitelisten – die Möglichkeit, nach einzelnen Einträgen zu suchen. Dabei können Sie nach verschiedenen Kriterien suchen, müssen aber nicht alle angeben. Lassen Sie bei der Suche eines der Felder leer, so werden *alle* Ergebnisse für dieses Feld angezeigt.

In der Übersicht kann man jetzt einzelne Mails durch einen Klick auf ② *'replay'* hinter der entsprechenden E-Mail erneut schicken. Bei einem Klick auf ③ *'umleiten'* kann die Mail auch an einen anderen Empfänger umgeleitet werden. Ist das Journal verfügbar, so kann durch einen Klick auf ④ *'anzeigen'* der entsprechende Eintrag im Journal eingesehen werden.

Gehen mehrere Mails verloren, so können diese ebenfalls erneut versendet werden. Hierzu schränken Sie zuerst die Ergebnismenge der Anzeige durch Eingabe von Absender (*'E-Mail-From'*), Empfänger (*'E-Mail-To'*) und/oder *'Empfangsdatum'* ein. Beim Empfangsdatum müssen Sie den Haken vor *'von'* bzw. *'bis'* setzen, damit die Einschränkung aktiv wird. Danach klicken Sie auf *'Anzeige erneuern'* und prüfen, ob Sie die richtigen Nachrichten ausgewählt haben. Ist dies der Fall, so klicken Sie auf ① *'Alle neu zustellen'* und alle ausgewählten Nachrichten werden – nach einer Sicherheitsabfrage – erneut versendet.

Informieren Sie Ihren Mail-Administrator, bevor Sie Mails erneut versenden, insbesondere, wenn es mehrere Mails auf einmal sind.

6.4 Warteschlange

Hier können Sie veranlassen, dass SPONTS versucht, alle Ihre Mails, die sich aktuell in der Warteschlange befinden, sofort auszuliefern. Im Zweifel sollten Sie dies mit Ihrem Mail-Administrator absprechen.

7 Bedienung der Web-GUI für den Administrator

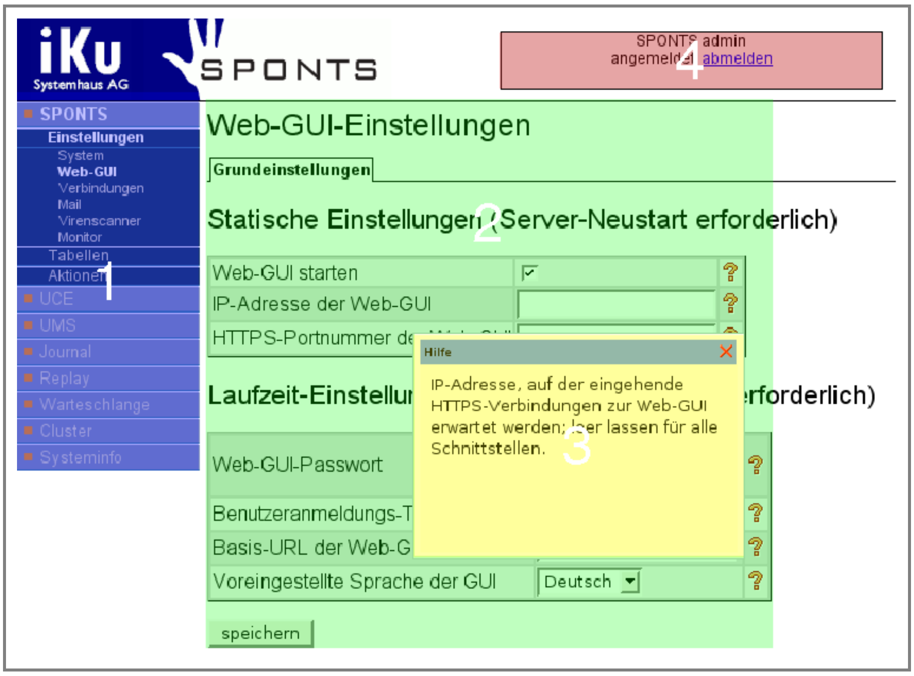


Abbildung 23: SPONTS Admin-Oberfläche

Die Oberfläche ist–- wie bei der Benutzerkonfiguration - in vier Bereiche aufgeteilt, die in obiger Abbildung einzeln markiert sind:

1 Navigation

2 Datenbereich

3 Hilfebereich (erscheint nur, wenn Hilfe zu einem Element ausgewählt wurde)

4 Login-Informationen/Link zum Abmelden

Die Navigation bleibt immer links im Bild. Der Datenbereich ändert sich, abhängig vom gewählten Navigationspunkt. Wenn Sie mit der Maus auf das Zeichen ? klicken, erscheint im Hilfebereich der entsprechende Hilfetext zu dieser Funktion. Hierzu muss in Ihrem Browser Java Script aktiviert sein. Der Hilfetext bleibt so lange stehen, bis Sie einen neuen Hilfetext auswählen, oder diesen mit einem Klick auf ✕ im Hilfebereich schließen.

Nachdem Sie Einstellungen auf einer Seite vorgenommen haben, müssen Sie diese mit *'speichern'* am Ende der Konfigurationsseite bestätigen.

Zur Konfiguration von SPONTS müssen Sie zuerst unter 'Empfänger' die gültigen Empfänger eingeben, sowie unter *'Einstellungen'* die Einstellungen ihres Netzwerkes angeben.

7.1 Wizards

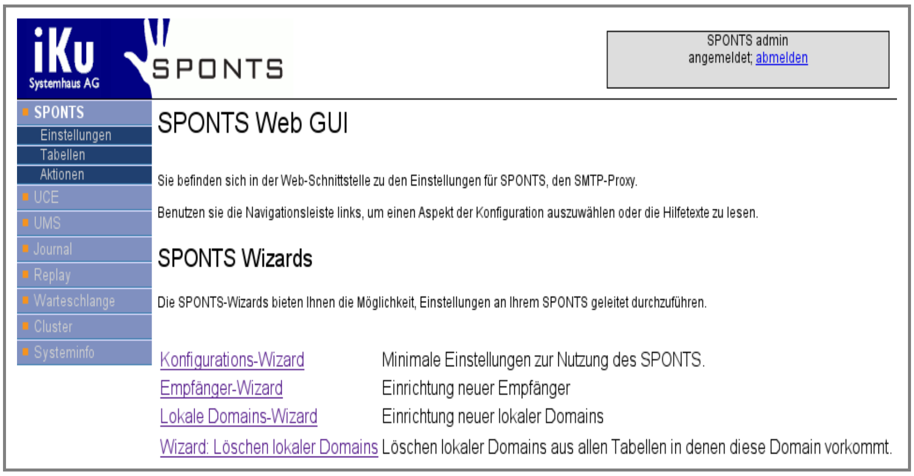


Abbildung 24 Wizards

Zur einfachen Konfiguration und Administration des SPONTS stehen Ihnen mehrere Wizards zur Verfügung. Über diese können Sie sich häufig wiederholende Aufgaben der Administration Ihres SPONTS einfach und komfortabel durchführen.

7.1.1 Konfigurations-Wizard

Der Konfigurations-Wizard dient der schellen und einfachen Einrichtung des SPONTS mit den minimalen Einstellungen, welche für den Betrieb nötig sind. Sollten Sie SPONTS neu einrichten, legen Sie ebenfalls gültige Empfänger und lokale Domains über die entsprechenden Wizards an.

Über den Konfiguration-Wizard können Sie die folgenden Einstellungen vornehmen:

- Absenderadresse für SPONTS-E-Mails (vgl. S. 38)
- Empfänger blockierter Anhänge (vgl. S. 38)
- Web-GUI-Passwort (vgl. S. 44)
- Basis-URL der Web-GUI (vgl. S. 45)
- Maximale E-Mail-Größe (vgl. S. 47)
- Empfänger-Überprüfung über SQL aktivieren (vgl. S. 47)
- Backend-Check aktivieren (vgl. S. 48)
- Liste vertrauenswürdiger Netzwerke (vgl. S. 49)
- Backend-Servername (vgl. S. 49)
- Backend-SMTP-Portnummer (vgl. S. 49)

Alle Einstellungen, welche Sie über diesen Wizard vornehmen sind Laufzeit-Einstellungen und sofort nach erfolgreichem Beenden des Wizards verfügbar.

7.1.2 Empfänger-Wizard

Über den Empfänger-Wizard können Sie neue gültige Empfänger komfortabel in mehreren Tabellen einrichten.



Abbildung 25: Empfänger-Wizard

Um neue Empfänger über den Empfänger-Wizard anzulegen, tragen Sie eine Empfängeradresse oder @Domain für eine ganze Domain als gültige Empfänger ein (vgl. dazu 7.3.1 Empfänger, S. 56).
Zusätzlich können Sie den oben angegebenen Empfänger durch den Wizard in die Liste der

- Empfänger statistischer E-Mails (vgl. 7.3.11 Statistik, S. 61)
- UCE-Einwilligung (vgl. 7.5.3 UCE Opt-In / UCE-Einwilligung, S. 73)
- Einwilligungen zur Nutzung von Wegwerfadressen (vgl. 7.5.4 Einwilligung zu Einwegadressen,S. 75)

durch Aktivierung der jeweiligen Optionsfelder eintragen lassen.

7.1.3 Lokale Domains Wizard

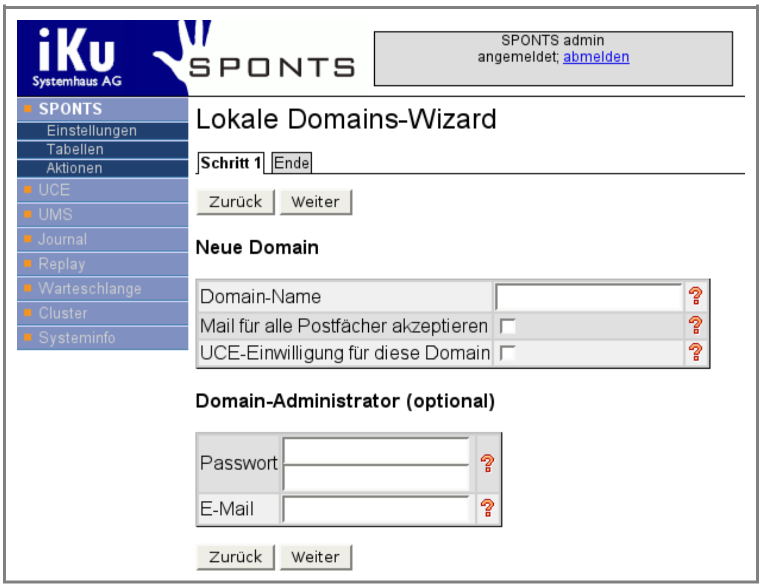


Abbildung 26: Lokale Domains-Wizard

Um eine neue lokale Domain zu erzeugen, starten Sie den Lokale Domains-Wizard und tragen Sie den Namen der Domain im Feld *Domain-Name* ein (vgl. dazu 7.3.2

Lokale Domains, S. 57).
Zusätzlich können sie die angegebene Domain über das Optionsfeld

- *Mail für alle Postfächer akzeptieren* in die Liste der gültigen Empfänger (vgl. 7.3.1 Empfänger, S. 56)
- *UCE-Einwilligung für diese Domain* in die Liste der UCE-Einwilligungen (vgl. 7.5.3 UCE Opt-In / UCE-Einwilligung, S. 73)

eintragen lassen.

Desweiteren können Sie durch Angabe eines geeigneten Passworts und einer E-Mail Adresse einen Domain-Administrator (vgl. 7.3.8 Domain-Admins, S. 60) für die angegebene Domain durch den Wizard anlegen lassen.

7.1.4 Wizard: Löschen lokaler Domains

Über diesen Wizard können sie eine lokale Domain und Empfänger, welche zu dieser Domain gehören aus den folgenden Tabellen entfernen:

- Lokale Domains
- Empfänger
- Statistik
- UCE Opt-In / UCE-Einwilligung
- Einwilligung zu Einwegadressen
- Domain-Admins

7.2 Einstellungen

Hier richten Sie SPONTS für Ihr Netzwerk ein.

Es gibt zwei Arten von Einstellungen:
1. statische Einstellungen
2. Laufzeit-Einstellungen
Bei Änderungen an den 'statischen Einstellungen' müssen Sie SPONTS über den Punkt *'Neustart'* (7.4.2 Neustart, S. 62) neu starten.

Um die minimalen Einstellungen zur Inbetriebnahme des SPONTS vorzunehmen, nutzen Sie den Konfigurations-Wizard und richten Sie Empfänger und Domänen über die entsprechenden Wizards ein.

Die jeweiligen SPONTS-Einstellungen sind unterteilt in Grund- und Erweiterte Einstellungen. Üblicherweise müssen lediglich Grundeinstellungen angepasst werden.

Als Einstellungstypen stehen statische und dynamische Einstellungen zur Verfügung.
Statische Einstellungen werden während des Systemstarts des SPONTS geladen. Nach Veränderungen an diesen Einstellungen müssen Sie SPONTS neu starten, damit diese wirksam werden.
Dynamische bzw. Laufzeit-Einstellungen werden während des Programmlaufs bei Bedarf ausgelesen. Veränderungen an diesen Einstellungen werden sofort wirksam, ein Neustart ist nicht notwendig.

Nachdem Sie Einstellungen auf einer Seite vorgenommen haben, müssen Sie diese mit *'speichern'* am Ende der Konfigurationsseite bestätigen.

7.2.1 Hinweise zur Eingabe

Einige der Einstellungen erfordern ein bestimmtes Format (Syntax). In vielen Fällen wird die Web-GUI sie auf eventuelle Eingabefehler hinweisen.

IP-Adressen und Netzwerke

Die Angabe erfolgt über Netznummer/Netzmaske (für Netzwerke) oder IP-Adresse (für einzelne Hosts), beides ist derzeit auf IPv4 begrenzt. Für die Netzmaske sind zwei Schreibweisen möglich: zum Beispiel 172.16.0.0/255.255.0.0 oder 172.16.0.0/16 für das Class B-Netz 172.16.x.x.

7.2.2 System

Menüpunkt: *'SPONTS →Einstellungen → System'*

Unter den Systemeinstellungen befinden sich allgemeine Einstellungen zum SPONTS.

Grundeinstellungen

Statische Einstellungen: Allgemein

- **SMTP-Bind-Adresse des SPONTS**
  IP-Adresse / Schnittstelle des SPONTS, auf der auf eingehende SMTP-Verbindungen gewartet wird. Lassen Sie diese Einstellung leer für alle Schnittstellen.
  Voreinstellung: leer (alle Schnittstellen)
- **SMTP-Portnummer des SPONTS**
  Port des SPONTS, auf dem eingehende SMTP-Verbindungen erwartet werden. Setzen Sie diese Einstellung auf `0`, um sie zu deaktivieren.
  Voreinstellung: `25`
- **SMTP/S-Portnummer des SPONTS**
  Port des SPONTS, auf dem eingehende SMTP/S-Verbindungen erwartet werden. Setzen Sie diese Einstellung auf `0`, um sie zu deaktivieren.
  Voreinstellung: `465`

Statische Einstellungen: Syslog Server

Hier befinden sich die Einstellungen zu einem verwendeten Syslog Server. Dieser kann die von SPONTS protokollierten Logs aufzeichnen.

- **Java-Loglevel**
  Java-Protokollierebene für Syslog. Alle Mitteilungen mit der eingestellten oder einer höheren Ebene werden protokolliert und an den Syslog Server weitergegeben.
  Voreinstellung: `INFO`
- **Syslog-Server**
  Protokollier (Syslog) Server, an den die zu protokollierenden Mitteilungen weitergegeben werden. Geben Sie hier die IP-Adresse oder den Namen des

entsprechenden Servers ein. Die Einstellung kann leer gelassen werden.
Voreinstellung: `'leer'`

- **Syslog-Portnummer**
  Portnummer, auf der ein konfigurierter Syslog-Server Verbindungen erwartet.
  Voreinstellung: `514`

Laufzeit-Einstellungen: System-Mail

Einstellungen zu den von SPONTS verschickten Systemmails.

- **Absenderadresse für SPONTS-E-Mails**
  Geben Sie hier die E-Mail Adresse ein, die als Absenderadresse verwendet wird, um automatisch generierte Mails (z.B. SPONTS Reports) zu versenden.

> Die voreingestellte Adresse sollte auf jeden Fall durch eine E-Mail Adresse eines Systembetreuers ersetzt werden.

  Voreinstellung: `sponts@invalid`

- **Empfänger blockierter Anhänge**
  Geben Sie hier die E-Mail Adresse an, an welche die entfernten Anhänge gesendet werden. Jeder entfernte Anhang wird in einer eigenen E-Mail an diese Adresse geschickt, wobei im Betreff dieser E-Mail die ID der E-Mail, die den Anhang enthielt, erscheint. Diese E-Mails enthalten nicht den Text der ursprünglichen Mail, sondern jeweils genau einen Anhang.
  Um einen Anhang einer E-Mail zuzuordnen, muss der hier angegebene Empfänger nur in den Betreffzeilen seiner E-Mails nach der Nachrichten-ID suchen, die in der ursprünglichen Mail enthalten ist. Diese kann er sich vom Benutzer, der den Anhang benötigt, mitteilen lassen.
  Die voreingestellte Adresse sollte auf jeden Fall durch eine E-Mail Adresse eines Systembetreuers ersetzt werden.
  Voreinstellung: admin@invalid

> **Warnung:** Anhänge, die auf diese Weise entfernt werden, werden nicht auf Viren geprüft! Benutzen Sie zum Abruf dieser E-Mails einen möglichst sicheren Mail-Client auf einem möglichst sicheren und virenresistenten Betriebssystem (z.B. Mozilla Thunderbird unter Linux).

Erweiterte Einstellungen

Statische Einstellungen: Allgemein

- **Dateiname der SPONTS-Lizenz**
  Vollständiger Pfad zu der Datei mit den Lizenzinformationen.
  Voreinstellung: `/system/etc/sponts/sponts-license.key`

- **JDBC-Treiberklasse**
  Verwendete JDBC-Treiberklasse. Geben Sie hier den vollständigen Java-Klassennamen an.
  Voreinstellung: `org.apache.derby.jdbc.EmbeddedDriver`

- **JDBC-URL**
  URL zum Zugriff auf die Datenbank.
  Voreinstellung: `jdbc:derby:SPONTS;create=false`

- **JDBC-Benutzername**
  Benutzername für JDBC-Zugriffe
  Voreinstellung: `sponts`
- **JDBC-Passwort**
  Passwort für JDBC-Zugriffe. Geben Sie das Passwort zur Überprüfung der korrekten Schreibweise in beide Eingabefelder ein.
- **Derby Datenverzeichnis**
  Verzeichnis für die Datenbankdateien von Derby.
  Voreinstellung: `/system/spool/sponts/db`
- **Derby-Netzwerkzugriff erlauben**
  Erlaube Verbindungen von außerhalb zur Derby Datenbank.
  Voreinstellung: `deaktiviert`
- **Derby-Bind Adresse**
  IP-Adresse, auf der eingehende Verbindungen zur Derby-Datenbank erwartet werden; leer lassen für alle Schnittstellen.
  Voreinstellung: `'leer'`
- **Derby-Port**
  Port, auf dem eingehende Verbindungen zur Derby-Datenbank erwartert werden.
  Voreinstellung: `1527`
- **DNS-Server**
  IP-Adresse des verwendeten DNS-Servers. Lassen Sie dieses Eingabefeld leer, um die Voreinstellung des System zu nutzen.
  Voreinstellung: `'leer'`
- **DNS-Cache TTL**
  Speicherdauer von Host-Einträgen im DNS-Cache. -1 bedeutet bis zum nächsten Neustart und 0 schaltet den Cache ab.
  Voreinstellung: `7200`
- **Kompletter Pfad der JSSE-Keystore-Datei**
  Vollständiger Pfad der Keystore-Datei, welche die Zertifikate/Schlüssel für SSL enthält.
  Voreinstellung: `/system/etc/sponts/sponts.keystore`
- **Höchstalter der Cache-Einträge (Sek.)**
  Maximales Alter der Einträge im Cache in Sekunden. Ältere Einträge werden gelöscht.
  Voreinstellung: `1209600` (14 Tage)

Laufzeit-Einstellungen: Allgemein

- **Temporäre(s) E-Mail Verzeichnis(se)**
  Eine Komma-getrennte Liste von Verzeichnissen, in denen E-Maildaten zwischengespeichert werden. Die Verzeichnisse sollten nur begrenzte Schreib-/Leseberechtigungen haben.
  Voreinstellung: `/system/spool/sponts`

- **Überlastschutz (Sek.)**
  Zeit, die zwischen SMTP-Data und einem OK des SPONTS gewartet wird. Der Überlastschutz sollte auf 60 Sekunden eingestellt sein.
  Voreinstellung: `60`
- **iKu-Timing-Whitelist aktivieren**
  Aktiviert die Weiße Liste für iKu-Timing. Die Aktivierung dieser Einstellung wird empfohlen.
  Voreinstellung: `aktiviert`
- **Prüfe fremde SSL-Zertifikate**
  Überprüfung fremder SSL-Zertifikate auf Vertrauenswürdigkeit. Hierzu muss das zu prüfende Zertifikat im SPONTS-Keystore oder von einer vertrauenswürdigen Autorität unterschrieben sein.
  Voreinstellung: `aktiviert`
- **Verzeichnis, in dem die Logdateien liegen**
  Pfadangabe des Verzeichnisses, in dem die Protokolldateien des SPONTS zu finden sind. Diese Angabe wird für den Export als Zip-Archiv (Backup) verwendet.
  Voreinstellung: `/system/log/sponts`
- **Volle Pfadangabe des Programms 'mysqldump'**
  Vollständige Pfadangabe des Kommandozeilen-Programms, welches die Datenbank im Backup sichert.
  Voreinstellung: `/system/mount/mysql/mysqldump`
- **Gesamte Kommunikation aufzeichnen (nur zur Fehlersuche!)**
  Diese Einstellung aktiviert das Protokollieren der kompletten SMTP-Kommunikation. Diese Einstellung sollten Sie nur zur Fehlersuche aktivieren.
  Voreinstellung: `deaktiviert`
- **Datei mit gültigen Empfänger-Domains**
  Vollständige Pfadangabe der Datei, die gültige Empfängerdomains enthält. Diese Datei muss jeweils eine Domain pro Zeile ohne '@' enthalten.
  Voreinstellung: `leer`
- **Liste der IKUC-berechtigten Netzwerke**
  Liste von IKUC-Netzwerken (zur Eingabe-Syntax siehe IP-Adressen und Netzwerke, Seite 37), von denen aus IKUC-Befehle ausgeführt werden können, beispielsweise durch den GenericProxy. Einträge werden durch Kommas oder Zeilenwechsel getrennt.
  Voreinstellung: `leer`

```
Beispiel:192.168.1.0/255.255.255.0,192.168.2.17/255.255.255.2
55
```

Laufzeit-Einstellungen: Cron

Cron ist ein Dienst des Betriebssystems, welcher zu festgelegten Zeiten Aktionen ausführt.

- **Startzeit von Cron**
  Startzeit der Cron-Aufträge. Die Zeit wird im Format 'hh:mm' angegeben.
  Voreinstellung: `03:15`

- **Cronjob-Latenz (Sek.)**
  Verzögerung (in Sekunden) zwischen Cron-Aufträgen, um andere Prozesse nicht zu lange zu blockieren.
  Voreinstellung: `300`

Laufzeit-Einstellungen: SMTP-Meldungen

Innerhalb des SMTP-Protokolls können für Benutzer verständliche Meldungen in Textform von SPONTS erzeugt werden. Diese Meldungen treten vorwiegend im Fall der Erkennung von UCE Blockierung einer empfangenen E-Mail auf und werden in vielen Fällen dem Absender von seinem Mailserver zugestellt.

- **Meldung beim Zurückweisen**
  Text, welcher mit einer SMTP-Antwort 450 oder 550 gesendet wird, wenn UCE erkannt und abgelehnt wird. Mögliche Meldungen sind: „mailbox unavailable“, „access denied“ oder „mailbox spam-protected“.
  Voreinstellung: `mailbox spam protected`
- **Meldung für Absender, die in der Schwarzen Liste sind**
  Text, welcher mit einer SMTP-Antwort 220, 221, 250, 450 oder 550 gesendet wird, wenn der Absender in der Schwarzen Liste eingetragen ist.
  Voreinstellung: `blacklisted`
- **Meldung, wenn ein Milter-Problem aufgetreten ist**
  Text, welcher mit der SMTP-Antwort 451 („local error“) gesendet wird. Diese Meldung tritt auf, wenn in einem Milter ein Ausnahmezustand aufgetreten ist und die Mail nicht verarbeitet werden konnte.
  Voreinstellung: `exception in milter`
- **Abschiedsmeldung**
  Abschiedsmeldung, welcher mit der SMTP-Antwort 221 als Reaktion auf SMTP-QUIT gesendet wird.
  Voreinstellung: `goodbye`
- **Meldung für Absender, die in der Weißen Liste sind**
  Text, welcher mit einer SMTP-Antwort 220, 221, 250 oder 354 gesendet wird, wenn der Absender einer E-Mail in der Weißen Liste steht.
  Voreinstellung: `whitelisted`
- **Meldung, wenn eine E-Mail dauerhaft abgewiesen wurde**
  Text, welcher mit der SMTP-Antwort 554 gesendet wird, wenn eine E-Mail abgelehnt wird.
  Voreinstellung: `you are blocked`
- **Meldung, wenn eine E-Mail vorübergehend abgewiesen wurde**
  Text, welcher mit einer SMTP-Antwort 451 gesendet wird, wenn eine E-Mail vorübergehend abgelehnt wird.
  Voreinstellung: `you are rejected`
- **Meldung nach Aufnahme in die Schwarze Liste**
  Text, welcher mit einer SMTP-Antwort 450 gesendet wird, wenn der Absender neu in die Schwarze Liste aufgenommen wurde.
  Voreinstellung: `you were blacklisted`

7.2.3 System-Mail Einstellungen

Menüpunkt: *'SPONTS → Einstellungen → System → Mails'*

Über die System-Mail Einstellungen können Sie die Textinhalte und Formate der durch SPONTS verschickten E-Mails konfigurieren. Diese E-Mails werden immer im Textformat erzeugt und Ihnen stehen Platzhalter zur Verfügung, um die relevanten Daten der jeweiligen SPONTS-Mail in eigene Texte einzubetten.

Grundeinstellungen

Laufzeit- Einstellungen: Benutzer-Login-Mails

Benutzer-Login-Mails werden an Benutzer verschickt, welche sich über ihre E-Mail Adresse am SPONTS anmelden wollen. Der Anmelde-Mechanismus des SPONTS für Benutzer sieht vor, dass diese eine E-Mail mit Anmeldelink zugeschickt bekommen, welcher für die über Benutzeranmeldungs-Timeout (Sek.) (S.45ff.) konfigurierbare Zeit gültig ist.

- **Betreffzeile**
  Betreffzeile der Anmelde-Mail. Für diese Betreffzeile stehen Ihnen zwei Platzhalter zur Verfügung:
  - *{0}: Login-Link:* Der Login-Link selbst wird in dieser Stelle eingefügt.
  - *{1}: Verfallsdatum:* Verfallsdatum des Anmeldelinks

  Voreinstellung:
  `SPONTS login link`
- **Mailtext**
  Mailtext der Anmelde-Mail. Dem Mailtext stehen die Platzhalter der Betreffzeile zur Verfügung.
  Voreinstellung:
  ```
  Use this link to login
  {0}
  It is valid until {1}.
  ```

Laufzeit-Einstellung: Attachment-Link-Mails

Attachment-Link-Mails werden an das über Empfänger blockierter Anhänge (S.38ff.) konfigurierte Postfach geschickt, falls E-Mailanhänge als zu blockierende Anhänge erkannt werden.

- **Betreffzeile**
  Betreffzeile der Attachment-Link-Mails, die der Sie die Möglichkeit haben, durch zwei Platzhalter die Mail-ID und den Dateinamen mit einfügen zu lassen.
  - *{0} : Mail-ID*
  - *{1} : Dateiname des Anhangs*

  Voreinstellung:
  `SPONTS attachment ID {0} ATTACHMENT {1}`

Die Attachment-Link-Mail selbst enthält den blockierten Anhang, welcher bei Bedarf an den eigentlichen Empfänger weitergereicht werden kann.

Laufzeit-Einstellung: Statistische E-Mails

Die statistischen E-Mails werden an den Administrator, die Domainadministratoren für ihre jeweile Domäne und alle Benutzer mit einer aktivierten Einwilligung für Statistiken täglich verschickt. Diese E-Mails enthalten Informationen über die Anzahl der empfangenen E-Mail, sowie detaillierte Tabellen über E-Mails, deren Empfang bzw. Versand nicht problemlos durchgeführt werden konnte.

- **Betreffzeile**
  Betreffzeile einer statistischen E-Mail mit den Platzhaltern:
  - *{0} : Empfängeradresse*
  - *{1} : Datum*

  Voreinstellung:
  `SPONTS report for {0} ({1})`
- **Mailtext**
  Der eigentliche Text einer statistischen E-Mail. Dieser Text wird im oberen Teil der Mail eingefügt und in jedem Fall dargestellt. Für den Mailtext steht eine Reihe von Platzhaltern zu Verfügung:
  - *{0} : Empfängeradresse*
  - *{1} : Datum*
  - *{2} : Anzahl zugestellter E-Mails*
  - *{3} : Anzahl der Mails in der Warteschlange*
  - *{4} : Anzahl abgebrochener Mailzustellungen*
  - *{5} : Anzahl blockierter E-Mails*
  - *{6} : Anzahl infizierter E-Mails (Viren)*
  - *{7} : Anzahl desinfizierter E-Mails (erfolgreich entfernte Viren)*
  - *{8} : Anzahl unzustellbarer E-Mails*

  Voreinstellung:
```
*** SPONTS daily mail report for {0} ***

Report for   {1}
delivered:   {2}
queued:      {3}
aborted:     {4}
blocked:     {5}
infected:    {6}
disinfected: {7}
undelivered: {8}
```
- **Kopfzeile der Tabellen**
  Nach dem Textkörper der statistischen E-Mail werden Tabellen zu allen Punkten des Textkörpers erzeugt, mit Ausnahme der zugestellten E-Mails. Für die Tabellen der als infizierten und desinfizierten E-Mails werden separate Tabellenköpfe definiert.
  - *{0} : Bezeichnung der Liste*

  Voreinstellung:
```
                Mails with status {0}:
Received From                          Subject
-------- -----------------------------
------------------------------
```
- **Kopfzeile der Tabelle der infizierten E-Mails**
  Kopfzeile der Tabelle der als infiziert erkannten E-Mails. Diese Kopfzeile enthält keine Platzhalter.
  Voreinstellung:
```
                Mails with status infected:
Received From                          Virus
```

```
-------- ------------------------------
------------------------------
```

- **Kopfzeile der Tabelle der desinfizierten E-Mails**
  Kopfzeile der Tabelle der erfolgreich desinfizierten E-Mails, d.h. E-Mails, welche von aktivierten Virenscannern erkannt wurden und aufgrund der aktivierten E-Mail Desinfektion (vgl. Infizierte Dateianhänge entfernen(Desinfektion), S. 52ff.) von diesen bereinigt werden konnten.
  Voreinstellung:

```
                Mails with status disinfected:
Received From                         removed Virus
-------- ------------------------------
------------------------------
```

Die Konfigurationsseite der System-Mail-Einstellungen besitzt neben dem Knopf *'speichern'* einen weiteren Knopf '*Einstellungen zurücksetzen*', über den Sie zuvor gesetzte Einstellungen dieser Seite auf den Auslieferungszustand zurücksetzen können. Dieses Zurücksetzen betrifft nur die Einstellungen auf dieser Seite, als Eintragungen werden die oben genannten Beispiele eingefügt.

7.2.4 Web-GUI

Menüpunkt: *'SPONTS →Einstellungen → Web-GUI*

Grundeinstellungen

Statische Einstellungen: Allgemein

- **Web-GUI starten**
  Legt fest, ob die grafische Web-Oberfläche (Web-GUI) gestartet werden soll. Nachdem die Web-GUI deaktiviert wurde, muss die entsprechende Einstellung von Hand in die Konfigurationsdatei des SPONTS eingetragen werden, um diese wieder zu aktivieren.
  Voreinstellung: `aktiviert`

Warnung: Nachdem der Start der Web-GUI deaktiviert wurde, kann dies nur noch über ein direktes Editieren der Einstellungsdatei des SPONTS rückgängig gemacht werden (vgl. 9.1 Reaktivierung der WEB-Gui nach vorheriger Deaktivierung, S.86).

- **IP-Adresse der Web-GUI**
  IP-Adresse, auf der eingehende HTTPS-Verbindungen zur Web-GUI erwartet werden. Lassen Sie diese Einstellung leer, um alle Schnittstellen zu nutzen.
  Voreinstellung: `'leer'`
- **HTTPS-Portnummer der Web-GUI**
  Port, auf dem eingehende HTTPS-Verbindungen zur Web-GUI erwartet werden.
  Voreinstellung: `8443`

Laufzeit-Einstellungen: Allgemein

- **Web-GUI Passwort**
  Administrator-Passwort für den Zugriff auf die Web-GUI. Geben Sie das Passwort in beide Felder ein, um Fehleingaben zu vermeiden.
  Voreinstellung:

- **Benutzeranmeldungs-Timeout (Sek.)**
  Haltbarkeitsdauer der Benutzerlogin-Schlüssel in Sekunden. Ist ein Schlüssel älter, als die hier angegebene Zeit, muss dieser einen neuen Login-Schlüssel über die Web-GUI anfordern und erhält einen aktuellen Login-Link zugeschickt.
  Voreinstellung: `28880` (8 Stunden)
- **Basis-URL der Web-GUI**
  Basis-URL für alle Links auf dem SPONTS-Server. Die Links sind nach folgendem Schema aufgebaut:
  `https://<sponts-hostname>:<port>/`
  Voreinstellung: https://sponts.invalid:8443/
- **Voreingestellte Sprache der GUI**
  Als Sprachen der Web-GUI können Sie Deutsch oder Englisch wählen. Diese Einstellung gilt für alle Benutzer, die sich an der Web-GUI anmelden.
  Voreinstellung: `Deutsch`

7.2.5 Eingehende Verbindungen

Menüpunkt: *'SPONTS →Einstellungen → Verbindungen→Eingehende Verbindungen'*

Grundeinstellungen

Laufzeit-Einstellungen: Allgemein

- **Maximalzahl eingehender Verbindungen**
  Maximale Anzahl gleichzeitiger eingehender Verbindungen zum SPONTS. Ist diese Anzahl erreicht, wird eine bestimmte Zeit auf das Freiwerden einer Verbindung gewartet. Sollte keine bestehende Verbindung frei werden, wird die eingehende Verbindung abgelehnt.
  Voreinstellung: `50`
- **Höchstzahl eingehender SMTP-Verbindungen je IP**
  Maximale Anzahl eingehender SMTP-Verbindungen von einer einzigen IP. Ist diese Anzahl erreicht, wird eine bestimmte Zeit auf das Freiwerden einer bestehenden Verbindung gewartet. Sollte dies nicht der Fall sein, wird die eingehende Verbindung abgelehnt.
  Voreinstellung: `10`
- **Pipelining erlauben**
  Diese Einstellung erlaubt den Einsatz von Pipelining. Pipelining beschleunigt die E-Mail Übertragung, durch den *Verzicht* auf Pipelining werden einige Spammer blockiert oder zumindest in ihrem E-Mail Versand verlangsamt.
  Voreinstellung: `deaktiviert`

Erweiterte Einstellungen

Laufzeit-Einstellungen: Allgemein

- **SMTP-Timeout (Sek.)**
  SMTP-Wartezeit (Timeout) in Sekunden. Untätige SMTP-Verbindungen werden nach dieser Wartezeit geschlossen. Empfohlen werden mindestens 120 Sekunden.
  Voreinstellung: `300` (5 Minuten)

- **Backlog Wartezeit (Sek.)**
  Wenn die maximale Anzahl eingehender Verbindungen erreicht ist, wird diese Zeit (in Sekunden) auf das Freiwerden einer bestehenden Verbindung gewartet, bevor die neue eingehende Verbindung getrennt wird.
  Voreinstellung: `10`

7.2.6 Ausgehende Verbindungen

Menüpunkt: *'SPONTS → Einstellungen → Verbindungen → Ausgehende Verbindungen'*

Grundeinstellungen

Laufzeit-Einstellungen: Allgemein

- **Höchstzahl gleichzeitiger Verbindungen zum Backend**
  Maximale Anzahl der Verbindungen, die gleichzeitig zum Backend hin geöffnet werden.
  Voreinstellung: `8`

7.2.7 Empfang

Menüpunkt: *'SPONTS → Einstellungen → Mail → Empfang'*

Diese Einstellungen betreffen den Empfang von E-Mails.

Grundeinstellungen

Laufzeit-Einstellungen: Allgemein

- **TLS für SMTP erlauben**
  Erlaubt per TLS (Transport Layer Security) verschlüsselte SMTP-Übertragung von E-Mails.
  Voreinstellung: `aktiviert`
- **TLS für POP3 erlauben**
  Erlaubt per TLS (Transport Layer Security) verschlüsselte POP3-Übertragung von E-Mails.
  Voreinstellung: `aktiviert`
- **TLS für IMAP erlauben**
  Erlaubt per TLS (Transport Layer Security) verschlüsselte IMAP-Übertragung von E-Mails.
  Voreinstellung: `aktiviert`
- **Kopfzeile X-Envelope-To hinzufügen**
  Fügt die Kopfzeile 'X-Envelope-To' zu jeder Mail hinzu. Diese Einstellung kann für Multidrop-Postfächer nötig sein.
  Voreinstellung: `deaktiviert`

Warnung: Durch aktivieren dieser Einstellung werden BCC-Empfänger (Blindkopien) sichtbar für alle Empfänger.

- **Vorhandene Received-Kopfzeilen entfernen**
  Alle vorhandenen Received-Header werden aus der Mail entfernt.
  Voreinstellung: `deaktiviert`

- **Received-Kopfzeile hinzufügen**
  SPONTS fügt eine Received-Kopfzeile in die Mail ein.
  Voreinstellung: `aktiviert`
- **Maximale E-Mail Größe (in Bytes)**
  Sollte das Backend über eine Größenbeschränkung für eingehende Mails verfügen, so muss hier ebenfalls eine Beschränkung angegeben werden. Diese muss kleiner als diejenige des Backends sein, damit sichergestellt ist, dass das Backend alle Mails akzeptiert. Die maximale zulässige E-Mail Gesamtgröße wird in in Bytes (ohne Kopfzeilen) angegeben. Ein Wert von 0 deaktiviert diese Einstellung, die E-Mail Größe wird dann nicht begrenzt.
  Voreinstellung: `0`
- **Höchstzahl der Hops**
  Höchstzahl von Mail-Hops (Server-Stationen), um Schleifen zu vermeiden.
  Voreinstellung: `25`
- **Höchstzahl der Empfänger**
  Maximale Anzahl der Empfänger für eine E-Mail Transaktion. Durch diese Einstellung können DOS-Angriffe (**D**enial **O**f **S**ervice) abgewehrt werden.
  Voreinstellung: `100`
- **Höchstzahl an Kopfzeilen**
  Maximale Anzahl an Kopfzeilen für eine Mail. Durch diese Einstellung können DOS-Angriffe abgewehrt werden.
  Voreinstellung: `1000`
- **Wartezeit zwischen Abrufversuchen (sec)**
  Gibt an, wie lange gewartet werden soll, bevor erneut alle in der Tabelle '*Abrufkonten*' eingetragenen POP3-Konten abgerufen werden. Die Angabe ist in Sekunden. Weniger als 10 Minuten sind nicht sinnvoll.
  Voreinstellung: `1800`

7.2.8 Weitergabe

Menüpunkt: *'SPONTS →Einstellungen → Mail→Weitergabe'*

Grundeinstellungen

Laufzeit-Einstellungen: Allgemein

- **Empfänger-Überprüfung über SQL aktivieren**
  Prüft die Empfänger einer Mail gegen die Tabellen 'Empfänger' und 'Lokale Domains'. Ist ein Empfänger oder seine Domain nicht in beiden Tabellen eingetragen, wird die E-Mail als unzustellbar abgelehnt.
  Voreinstellung: `aktiviert`

Laufzeit-Einstellungen: Backendcheck

Wenn SPONTS eingehende Nachrichten nicht zum Backend, sondern zu einem vorgeschalteten Server - beispielsweise einem Virus-Scanner - schicken soll, dann können Sie hier das eigentliche Backend einstellen. Der Backend-Check wird dann gegen das hier eingestellte Backend gemacht, die Nachricht selbst wird aber zum Viren-Scanner gesendet. Wenn Sie hier nichts eintragen, wird für den Check das eingestellte Backend verwendet.

- **Servername für Backendcheck**
  Name oder IP-Adresse des Backend-Servers für die Überprüfung der E-Mail Empfänger über das Backend. Wenn dieser Eintrag leer ist, wird das voreingestellte Backend genutzt.
  Voreinstellung: `'leer'`
- **SMTP-Portnummer für den Backendcheck**
  `SMTP-Port des Backends zur Überprüfung.`
  `Voreinstellung: 'leer'`
- **SSL zum Backendcheck benutzen**
  Die Verbindung zum Backend wird SSL-verschlüsselt aufgebaut.
  Voreinstellung: `deaktiviert`
- **Backendcheck aktivieren**
  Aktiviert die Überprüfung des Empfängers beim Backend. Diese Einstellung ist sinnvoll, wenn Sie nicht jeden gültigen Empfänger einzeln in die SQL-Tabelle eintragen wollen. Durch den Backendcheck werden nur E-Mails weitergeleitet, deren Empfänger dem Backend bekannt sind. Diese Einstellung sollte aktiviert werden, wenn das Backend nur bestimmte Adressen empfängt, damit keine Mails auf der SPONTS-Box wegen Unzustellbarkeit liegen bleiben.
  Voreinstellung: `aktiviert`

> Sollte das Backend ausfallen, so werden in dieser Zeit **alle** Empfängeradressen akzeptiert, damit keine Nachricht verloren geht.

Laufzeit-Einstellungen: Authentifizierung

Mittels SMTP-Authentisierung können Clients von jeder beliebigen IP-Adresse aus eine Mail über SPONTS versenden (Relay). Die Authentisierung stellt sicher, dass nur berechtigte Clients dies können. Diese erfolgt über Benutzername und Passwort, wobei die folgenden Verfahren zur Verfügung stehen:

- *PLAIN (Klartext)*
- *LOGIN (Klartext)*
- *CRAM-MD5 (Verschlüsselt)*
- *CRAM-SHA1 (Verschlüsselt)*

Die Benutzerdaten können entweder in der Tabelle *'Benutzer'* (7.3.10 Benutzer, S. 61) abgelegt oder gegen das Backend geprüft werden. Ist die Prüfung gegen das Backend aktiv, so werden die Zugangsdaten gegen das Backend und die Tabelle *'Benutzer'* geprüft. Ist der Benutzer in einem der beiden vorhanden, wird der Zugriff erlaubt.

- **SMTP-AUTH PLAIN erlauben**
  Erlaubt die SMTP-Authentisierungsmethode PLAIN.
  Voreinstellung: `aktiviert`
- **SMTP-AUTH LOGIN erlauben**
  Erlaubt die SMTP-Authentisierungsmethode LOGIN.
  Voreinstellung: `aktiviert`
- **SMTP-AUTH CRAM-MD5 erlauben**
  Erlaubt die SMTP-Authentisierungsmethode CRAM-MD5.
  Voreinstellung: `aktiviert`

- **SMTP-AUTH CRAM-SHA1 erlauben**
  Erlaubt die SMTP-Authentisierungsmethode CRAM-SHA1.
  Voreinstellung: `aktiviert`
- **Überprüfe SMTP-Auth gegen Backend**
  Die SMTP-Authentifizierung wird gegen das Backend geprüft.
  Voreinstellung: `deaktiviert`

Laufzeit-Einstellungen: Authentifizierung über IP-Adressen

- **Liste vertrauenswürdiger Netzwerke (relaying erlaubt)**
  Rechner aus Netzwerken, welche in dieser Liste eingetragen sind (zur Eingabe-Syntax siehe IP-Adressen und Netzwerke, Seite 37), dürfen E-Mails ohne UCE-Prüfung an externe Domains senden. Die Einträge der Liste werden durch Kommas oder Zeilenwechsel getrennt angegeben. Eine Datei, bzw. einen Pfad zu einer Datei mit diesen Informationen können Sie an dieser Stelle nicht eintragen.
  Voreinstellung: `'leer'`

Erweiterte Einstellungen

Laufzeit-Einstellungen: Allgemein

- **Zeitfenster für Anmeldung durch SMTP-nach-POP/IMAP (Sek.)**
  Zeitfenster für SMTP-Zugriffe nach erfolgreicher POP/IMAP-Anmeldung. 0 deaktiviert SMTP nach POP/IMAP.
  Voreinstellung: `300` (5 Minuten)

7.2.9 Versand

Menüpunkt: *'SPONTS → Einstellungen → Mail → Versand'*

Grundeinstellungen

Laufzeit-Einstellungen: Backend

- **Backend-Servername**
  Name des Servers an den eingehende E-Mails weitergeleitet werden. Geben Sie hier den Namen oder die IP-Adresse Ihres Backends an.
  Voreinstellung: `smtp.invalid`
- **Backend-SMTP-Portnummer**
  Portnummer des Backend-Servers.
  Voreinstellung: `25`
- **SSL zum Backend benutzen**
  Durch aktivieren dieser Einstellung werden die Verbindungen zum Backend über eine SSL-Verschlüsselung aufgebaut.
  Voreinstellung: `deaktiviert`
- **Authentifizierung**
  Methode der Authentifizierung am Backend.

  - *PLAIN*
  - *Login*
  - *CRAM-MD5*
  - *CRAM-SHA1*

  Bei Verwendung von PLAIN oder Login reicht SPONTS die eingehende SMTP-AUTH-Daten (Login/Passwort) jeweils an das Backend weiter.
  Bei den verschlüsselten Methoden CRAM-MD5 und CRAM-SHA1 ist dies prinzipbedingt nicht möglich und es werden Default-Zugangsdaten verwendet (s.u.).
  Voreinstellung: `PLAIN`

- **Login** / **Passwort**
  Default-Zugangsdaten für SMTP-AUTH am Backend. Tragen Sie hier eine feste Login/Passwort-Kombination für SMTP-AUTH am Backend ein, wenn
  - CRAM-MD5 oder CRAM-SHA1 verwendet wird.
  - oder wenn SPONTS über die Tabelle '*Benutzer*' authentifiziert, am Backend aber trotzdem SMTP-AUTH verwendet wird.

  Voreinstellung: `leer`

Laufzeit-Einstellungen: Smarthost

- **Smarthost Servername**
  Hier geben Sie (falls vorhanden), den Hostnamen oder die IP-Adresse und die Portnummer des Mailservers an, über den per SMTP alle ausgehenden E-Mails gesendet werden. Lassen Sie diese Einstellung leer, wenn kein Smarthost verwendet werden soll.
  Voreinstellung: `'leer'`
- **Smarthost SMTP-Portnummer**
  SMTP-Port des Servers, an den ausgehende E-Mails weitergesendet werden.
  Voreinstellung: `'leer'`
- **SSL zum Smarthost verwenden**
  Die Verbindung zum Smarthost wird SSL-Verschlüsselt aufgebaut.
  Voreinstellung: deaktiviert

Erweiterte Einstellungen

Laufzeit-Einstellungen: Warteschlange

- **Mindestalter in der Warteschlange (Sek.)**
  Mindestalter der nicht zustellbaren E-Mails (in Sekunden), bevor der nächste Sendeversuch unternommen wird.
  Voreinstellung: `300` (5 Minuten)
- **Wartezeit zwischen Sendeversuchen (Sek.)**
  Wartezeit nach einem erfolglosen Zustellversuch einer E-Mail. Nach dieser Wartezeit wird ein weiterer Sendeversuch unternommen. RFC 1123 empfiehlt mindestens 30 Minuten = 1800 Sekunden.
  Voreinstellung: `1800` (30 Minuten)
- **Maximale gesamte E-Mail Zustellungsdauer (Sek.)**
  Zeitdauer, wie lange insgesamt versucht werden soll, eine E-Mail zu versenden, bevor der Versuch aufgegeben wird und der Absender eine

Meldung über die Unzustellbarkeit der E-Mail bekommt. RFC 1123 empfiehlt mindestens 4-5 Tage = 345600-43200 Sekunden.
Voreinstellung: `432000`

- **Block-Zeit für lahme Server (Sek.)**
  Wenn ein SMTP-Server zeitweise keine E-Mails akzeptiert, wird dieser für die eingestellte Zeit für den Versand gesperrt. 0 deaktiviert die Sperrung lahmer Server.
  Voreinstellung: `1800` (30 Minuten)

7.2.10 Signatur

Grundeinstellungen

Menüpunkt: *'SPONTS →Einstellungen → Mail→Signatur'*

Laufzeit-Einstellungen:

- **Anhängen der Signatur**
  Mit diesem Schalten können Sie das automatische Anhängen von Signaturtexten an jede E-Mail aktivieren oder deaktivieren.
- **Signatur**
  Der hier angegebene Text wird an alle Emails angehängt.
- **HTML-Signatur**
  Der hier angegebene HTML-Text wird an alle HTML-Emails angehängt.

7.2.11 Virenscanner

Grundeinstellungen

Menüpunkt: *'SPONTS →Einstellungen → Virenscanner'*

Laufzeit-Einstellungen: Allgemein

- **Vorgehen bei Mailbomben**
  Vorgehen, sobald die Grenzwerte für E-Mail Bomben überschritten werden. Als Vorgehen stehen folgende Einstellungen zur Auswahl:
  - *annehmen*
    Trotz einer erkannten Mailbombe wird die E-Mail ohne Virenprüfung angenommen
  - *ablehnen*
    Die E-Mail wird mit einer Fehlermeldung abgelehnt.
    Voreinstellung: `annehmen`
- **AntiVir aktivieren**
  Aktivierung des Virenscanners AntiVir.
  Voreinstellung: `deaktiviert`
- **Sophos aktivieren**
  Aktiviert den Virenscanner Sophos.
  Voreinstellung: `deaktiviert`

Erweiterte Einstellungen

Laufzeit-Einstellungen: Allgemein

- **Maximale Größe des Archiv Inhalts**
  Maximale Größe dekomprimierter Archive in Bytes. Diese Einstellung dient der Erkennung von Mailbomben.
  Voreinstellung: `100000000`
- **Maximale Rekursion in Archive**
  Maximale Rekursionstiefe bei Archiven. Diese Einstellung dient der Erkennung von Mailbomben.
  Voreinstellung: `6`
- **Maximales Verhältnis unkomprimiert:komprimiert**
  Maximales Verhältnis von dekomprimierten zu komprimierten Daten. Diese Einstellung dient der Erkennung von Mailbomben.
  Voreinstellung. `150`
- **Max. Anzahl an Virenscannern**
  Maximale Anzahl der gleichzeitig laufenden Virenscanner-Instanzen.
  Voreinstellung: `2`
- **Wartezeit auf verfügbare Scanner (Sek.)**
  Sobald die maximale Anzahl der parallel laufenden Virenscannern erreicht ist, wird diese Zeit (in Sekunden) auf das Freiwerden eines Scanners gewartet, bevor die Verbindung getrennt wird.
  Voreinstellung: `240`
- **Infizierte Dateianhänge entfernen(Desinfektion)**
  Durch die Aktivierung dieser Einstellung wird versucht, infizierte Dateianhänge aus einer E-Mail zu entfernen. Nach dieser Desinfektion wird die betreffende E-Mail erneut auf Virenbefall geprüft. Sollten die Virenscanner selbst nach der Desinfektion als infiziert erkannt, wird diese von SPONTS abgelehnt. Andernfalls wird die E-Mail an den Empfänger weitergeleitet, und im Inhalt der E-Mail wird vermerkt, dass ein Virus entfernt worden ist. Diese Desinfektion wird jedoch nur für Benutzer oder Domains durchgeführt, welche eine Einwilligung in der Einwilligungsliste (7.3.12 Virenscanner / E-Mail Desinfektion, S.61) haben.
  Voreinstellung: `deaktiviert`

Laufzeit-Einstellungen: H+BEDV AntiVir

- **Servername für AntiVir**
  Name des Servers, auf dem AntiVir läuft. Sollte AntiVir lokal auf dem SPONTS laufen, geben Sie hier bitte `'localhost'` an.
  Voreinstellung: `localhost`
- **Portnummer des SAVAPI von AntiVir**
  SAVAPI-Port von AntiVir.
  Voreinstellung: `9753`

Laufzeit-Einstellungen: Sophos SAVI via Sophie

- **Socket-Name von Sophie**
  Name des Unix-Domain-Sockets, um die Verbindung zu Sophie aufzubauen.
  Voreinstellung: `/system/spool/sophos/sophie`

Laufzeit-Einstellungen: Kaspersky via aveclient

- **Socket-Name von Kaspersky**
  Name des Unix-Domain-Sockets, um die Verbindung zu aveclient aufzubauen.
  Voreinstellung: `/system/spool/kav/aveserver`

7.2.12 Monitor

Menüpunkt: *'SPONTS →Einstellungen → Monitor'*

Grundeinstellungen

Statische Einstellungen: Allgemein

- **POP3-Bind-Adresse von SPONTS/Monitor**
  IP-Adresse, auf der eingehende POP3-Verbindungen erwartet werden. Lassen Sie diese Einstellung leer, wenn alle Schnittstellen des SPONTS genutzt werden sollen
  Voreinstellung: `127.0.0.1`
- **POP3-Portnummer von SPONTS/Monitor**
  Port, auf dem eingehende POP3-Verbindungen erwartet werden. Der Wert 0 deaktiviert das Monitoring für POP3.
  Voreinstellung: `18110`
- **POP3/S-Portnummer von SPONTS/Monitor**
  Port, auf dem eingehende POP3/S-Verbindungen erwartet werden. Der Wert 0 deaktiviert das Monitoring für POP3/S.
  Voreinstellung: `18995`
- **IMAP-Bind-Adresse von SPONTS/Monitor**
  IP-Adresse, auf der eingehende IMAP-Verbindungen erwartet werden. Lassen Sie diese Einstellung leer, wenn alle Schnittstellen des SPONTS genutzt werden sollen.
  Voreinstellung: `127.0.0.1`
- **IMAP-Portnummer von SPONTS/Monitor**
  Port, auf dem eingehende IMAP-Verbindungen erwartet werden. Der Wert 0 deaktiviert das Monitoring für IMAP.
  Voreinstellung: `18143`
- **IMAP/S-Portnummer von SPONTS/Monitor**
  Port, auf dem eingehende IMAP/S-Verbindungen erwartet werden. Der Wert 0 deaktiviert das Monitoring für IMAP/S.
  Voreinstellung: `18993`

Laufzeit-Einstellungen: Allgemein

- **Betreiberkennung**
  Betreiberkennung, wie sie von der RegTP zugewiesen wurde.
- **Administrator-Adresse**
  E-Mail Adresse für Benachrichtigungen in Problemfällen des SPONTS/Monitor.

Erweiterte Einstellungen

Laufzeit-Einstellungen: Allgemein

- **Anzahl vorgeschalteter Mailserver im Sandwich-Mode**
  Anzahl der vor dem SPONTS vorgeschalteten Mailserver, wenn SPONTS/Monitor im Sandwich-Mode betrieben wird.
- **Temporäres Verzeichnis für SPONTS/Monitor**
  Dieses Verzeichnis darf nicht für alle lesbar sein, da es E-Maildaten enthalten wird.

Monitor – POP3

Menüpunkt: *'SPONTS →Einstellungen → Monitor→ POP3*

Grundeinstellungen

Laufzeit-Einstellungen: Allgemein

- **POP3-Server im Backend**
  IP-Adresse oder Name des POP3-Servers im Backend.
  Voreinstellung: `localhost`
- **POP3-Portnummer im Backend**
  Port des POP3-Servers im Backend.
  Voreinstellung: `110`
- **SSL zum POP3-Backend verwenden**
  Die POP3-Verbindung zum Backend wird SSL-verschlüsselt aufgebaut.
  Voreinstellung: `deaktiviert`
- **Höchstzahl eingehender POP3-Verbindungen je IP**
  Maximale Anzahl eingehender POP3-Verbindungen von einer einzelnen IP-Adresse. Sobald diese Verbindungszahl erreicht ist, wird keine weitere eingehende POP3-Verbindung akzeptiert, bis bestehende Verbindungen von dieser IP-Adresse freigegeben werden.
  Voreinstellung: `10`

Erweiterte Einstellungen

Laufzeit-Einstellungen: Allgemein

- **Maximalzahl eingehender POP3-Verbindungen**
  Maximale Anzahl gleichzeitig eingehender POP3-Verbindungen von unterschiedlichen IP-Adressen.
  Voreinstellung: `50`
- **POP3 Backlog Wartezeit (Sek.)**
  Wenn die maximale Anzahl an eingehenden POP3-Verbindungen von unterschiedlichen IP-Adressen erreicht ist, wird diese Zeit (in Sekunden) auf das Freiwerden einer bestehenden Verbindung gewartet, bevor die neue eingehende Verbindung getrennt wird.
  Voreinstellung: `10`

Monitor – IMAP

Menüpunkt: *'SPONTS →Einstellungen → Monitor→ IMAP*

Grundeinstellungen

Laufzeit-Einstellungen: Allgemein

- **IMAP-Server im Backend**
  IP-Adresse oder Name des IMAP-Servers im Backend.
  Voreinstellung: `localhost`
- **IMAP-Portnummer im Backend**
  Port des IMAP-Servers im Backend.
  Voreinstellung: `143`
- **SSL zum IMAP-Backend verwenden**
  Die IMAP-Verbindung zum Backend wird SSL-verschlüsselt aufgebaut.
  Voreinstellung: `deaktiviert`
- **Gemeinsames Verzeichnis auf dem IMAP-Server**
  Gemeinsames Verzeichnis auf dem IMAP-Server, welches bei Kopieroperationen mit überwacht werden soll.
  Voreinstellung: `users`
- **Höchstzahl eingehender IMAP-Verbindungen je IP**
  Maximale Anzahl eingehender IMAP-Verbindungen von einer einzelnen IP-Adresse. Sobald diese Verbindungszahl erreicht ist, wird keine weitere eingehende IMAP-Verbindung akzeptiert, bis bestehende Verbindungen von dieser IP-Adresse freigegeben werden.
  Voreinstellung: `10`

Erweiterte Einstellungen

Laufzeit-Einstellungen: Allgemein

- **IMAP-Timeout (Sek.)**
  IMAP-Zeitüberschreitung. RFC2060, Abschnitt 5.4 schreibt mindestens 30 Minuten (1800 Sekunden) vor.
  Voreinstellung: `1800`
- **Maximale Anzahl eingebender IMAP-Verbindungen**
  Maximale Anzahl gleichzeitig eingehender IMAP-Verbindungen von unterschiedlichen IP-Adressen.
  Voreinstellung: `50`
- **IMAP Backlog Wartezeit (Sek.)**
  Wenn die maximale Anzahl an eingehenden IMAP-Verbindungen von unterschiedlichen IP-Adressen erreicht ist, wird diese Zeit in Sekunden auf das Freigegeben einer bestehenden Verbindung gewartet, bevor die neue eingehende Verbindung getrennt wird.
  Voreinstellung: `10`

Monitor - FTP

Menüpunkt: *'SPONTS →Einstellungen → Monitor→ FTP*

Grundeinstellungen

Laufzeit-Einstellungen: Allgemein

- **Höchstzahl gleichzeitiger FTP-Verbindungen**
  Maximale Anzahl gleichzeitiger FTP-Verbindungen zur Ausleitung von E-Mail Daten.
  Voreinstellung: `8`

Erweiterte Einstellungen

Laufzeit-Einstellungen: Allgemein

- **Wartezeit zwischen FTP-Versuchen (Sek.)**
  Wartezeit zwischen zwei FTP-Sendeversuchen.
  Voreinstellung: `300` (5 Minuten)
- **Mindestalter von FTP-Dateien vor Neuversuch (Sek.)**
  Mindestalter von E-Mail Dateien auf der Festplatte, bevor ein neuer Sendeversuch über FTP unternommen werden soll.
  Voreinstellung: `300` (5 Minuten)
- **FTP-Proxy Host**
  Hostname des FTP-Proxys. Lassen Sie diese Einstellung leer, wenn kein Proxy verwendet wird.
  Voreinstellung: `'leer'`
- **FTP-Proxy Port**
  Port des FTP-Proxys.
  Voreinstellung: `'leer'`
- **FTP-Proxy Benutzername**
  Benutzername zur Anmeldung am FTP-Proxy.
  Voreinstellung: `'leer'`
- **FTP-Proxy Passwort**
  Passwort zur Anmeldung am FTP-Proxy.
  Voreinstellung: `'leer'`

7.3 Tabellen

Hier befinden sich alle in Tabellenform gefassten Konfigurationen des SPONTS, wie Empfänger- und Domainlisten oder Filterungen nach E-Mail-Envelope und Anhängen.

Die jeweiligen Tabellen haben in ihren Kopfzeilen Felder zur Filterung. Um nach Begriffen zu filtern, geben Sie diesen in das entsprechende Feld ein und drücken Sie die Eingabetaste. Die Begriffe müssen Sie nicht mit '*' angeben, wenn Sie nur Teilworte von gesuchten Begriffen suchen wollen.

Um neue Einträge in einer Liste zu erzeugen, Klicken Sie auf den Link 'neuer Eintrag' im rechten Teil der Kopfzeile einer Tabelle. Über diesen Link gelangen Sie zu einer Eingabeseite zu den Einträgen der gewählten Tabelle.

7.3.1 Empfänger

Menüpunkt: *'SPONTS → Tabellen → Empfänger'*

Hier geben Sie die gültigen Empfängeradressen an. Sie können sowohl einzelne Benutzer im Format 'benutzer@domain', als auch komplette Domains im Format '@domain' angeben.
SPONTS nimmt nur E-Mails für Empfänger oder Domains an, die in dieser Liste eingetragen sind. Bei E-Mails an Empfänger, die nicht in dieser Liste eingetragen sind, wird die Annahme verweigert.

> Wenn Sie eine komplette Domain angeben, dann werden auch E-Mails mit Zieladresse '"benutzer@anderedomain"@domain' akzeptiert. Stellen Sie sicher, dass Ihr Backend solche Mails nicht an 'benutzer@anderedomain' weiterleitet, damit Sie kein offenes Relay haben.

7.3.2 Lokale Domains

Menüpunkt: *'SPONTS → Tabellen → Lokale Domains'*

Tragen Sie hier – auch wenn bei *'Empfänger'* schon angegeben – alle Domains ein, für die SPONTS E-Mail empfangen soll.
SPONTS nimmt nur E-Mails für die in dieser Liste angegebenen Domains an. Bei E-Mails an Domains, die nicht in dieser Liste eingetragen sind, wird die Annahme verweigert.

7.3.3 Abrufkonten (POP3)

Menüpunkt: *'SPONTS → Tabellen → Abrufkonten*

Hier können Sie alle POP3-Server eintragen, von denen in regelmäßigen Abständen (siehe *Einstellungen → Mail → Empfang → Wartezeit zwischen Abrufversuchen*) Emails abgerufen werden sollen. Der Standard-Port für POP3 ist 110 (995 bei Verwendung von SSL).

Wählen Sie die Option 'SSL - Zertifikat gültig' nur dann aus, wenn sie das SSL-Zertifikat des POP3-Servers korrekt im SPONTS-Keystore eingetragen haben (siehe 4.4 Zertifikate).

Als Empfänger geben Sie die Email-Adresse an, an die die abgerufenen Emails weitergeleitet werden sollen.

Unter 'Index des Empfangs-Servers' geben Sie an, den wievielten Received-Header SPONTS verwenden soll, um den ürsprünglichen Absende-Server zu ermitteln. Der Wert ist 0-basiert, d.h. wenn Sie 0 angeben wird der erste Header ausgewertet, usw.

7.3.4 Empfänger ersetzen

Menüpunkt: *'SPONTS → Tabellen → Empfänger ersetzen'*

Hier können Sie Empfängeradressen von SPONTS umschreiben lassen. Tragen Sie dazu einzelne E-Mail Adressen oder ganze Domains ein, welche umgeschrieben werden sollen.
Hier haben Sie die über die Einstellung 'Modus' die Möglichkeit, die Empfängeradresse einer E-Mail umschreiben zu lassen, oder eine Kopie der E-Mail an eine andere Adresse senden zu lassen.

7.3.5 Backend je Empfänger

Menüpunkt: *'SPONTS → Tabellen → Backend je Empfänger'*

An dieser Stelle können Sie für Ihre E-Mail Empfänger unterschiedliche Backends eintragen. Um ein empfängerspezifisches Backend am SPONTS einzurichten, müssen Sie zumindest die Empfänger E-Mail oder eine Domain, die IP-Adresse des Backends und dessen Portnummer eintragen.
Eine sichere Kommunikation zwischen SPONTS und dem jeweiligen Backend können Sie über SSL erzwingen und es besteht die Möglichkeit der Authentifizierung mit Login und Passwort am gewählten Backend.

7.3.6 Envelope

Menüpunkt: *'SPONTS → Tabellen → Envelope'*

Mit dem '*Vorgehen nach SMTP-Envelope*' können Sie die normale Spam-Bewertung umgehen und beliebig viele feste Vorgehensweisen definieren. Als Kriterien stehen Ihnen hierbei

- *'Absender-IP'*
- *'Absender'*
- *'Empfänger'*

zur Verfügung. Sie müssen mindestens eines davon angeben. Als Vorgehensweise haben Sie die Wahl zwischen

- *'annehmen' / 'accept'*
  Nachrichten werden immer angenommen.
- *'ablehnen' / 'reject'*
  Nachrichten werden immer abgewiesen.
- *'niemals zurückweisen' / 'never-reject'*
  Nachricht niemals zurückweisen, die eingehenden E-Mails werden jedoch auf Viren geprüft.
- *'nicht auf Viren prüfen' / 'noscan'*
  Nachrichten werden ohne Virenprüfung verarbeitet, eine Spam-Prüfung wird jedoch vorgenommen.
- *'erlaube verschlüsselte Dateien*
  Diese Einstellung verhindert, dass E-Mails mit verschlüsselten Dateien, welche nicht von den Virenscannern geprüft werden können, abgewiesen werden. Eine Prüfung auf Spam wird hingegen durchgeführt.
- *'Immer annehmen, nicht auf Viren prüfen'*
  Eingehende E-Mails werden immer angenommen. Es wird keine Spam- oder Virenprüfung vorgenommen.
- *'Postfach ist eine Spamfalle'*
  Diese Einstellung dient der Nutzung von Spamfallen (Teergruben). Durch diese Einstellung wird der versendende Server im Sendevorgang blockiert. Die Einstellungen hierzu finden Sie unter 7.5.1 Proaktive Anti-UCE Maßnahmen,S. 72ff.

Beispiele

Alle Nachrichten eines Absenders (z.B. Newsletter) durchlassen

IP-Adresse des Absenders	leer
Absender E-Mail oder @domain	eintragen
Empfänger E-Mail oder @domain	leer
Vorgehen	*'E-Mail annehmen' / 'accept'*

Alle Nachrichten an einen Empfänger durchlassen

IP-Adresse des Absenders	leer
Absender E-Mail oder @domain	leer
Empfänger E-Mail oder @domain	eintragen
Vorgehen	*'E-Mail annehmen' / 'accept'*

Absende-Domain komplett freischalten (z.B. Kunde)

IP-Adresse des Absenders	leer
Absender E-Mail oder @domain	@domainname
Empfänger E-Mail oder @domain	eintragen
Vorgehen	*'E-Mail annehmen' / 'accept'*

Spam-Server sperren

IP-Adresse des Absenders	eintragen
Absender E-Mail oder @domain	leer
Empfänger E-Mail oder @domain	eintragen
Vorgehen	*'E-Mail ablehnen' / 'reject'*

Absender sperren

IP-Adresse des Absenders	leer
Absender E-Mail oder @domain	eintragen
Empfänger E-Mail oder @domain	leer
Vorgehen	*'E-Mail ablehnen' / 'reject'*

Bestimmten Absender an bestimmten Empfänger freischalten

IP-Adresse des Absenders	leer
Absender E-Mail oder @domain	eintragen
Empfänger E-Mail oder @domain	eintragen
Vorgehen	*'E-Mail annehmen' / 'accept'*

7.3.7 Anhang

Menüpunkt: *'SPONTS → Tabellen → Anhang'*

Über die Anhang-Filter Liste kann SPONTS bestimmte Dateianhänge in E-Mails von einem Absender oder an einen Empfänger durchlassen oder entfernen. Wird ein Anhang von einer E-Mail entfernt, so bleibt die E-Mail ansonsten unverändert. Lediglich der Anhang wird durch einen Hinweis ersetzt, der den Dateinamen des Anhangs sowie eine Identifikationsnummer (ID) enthält. Über diese

Identifikationsnummer können Benutzer den Anhang bei ihrem Administrator anfordern.
Die durch den Administrator erzeugten Anhang-Filter werden vor Anhang-Filtern der Benutzer verarbeitet und können diese so übergehen.

Als Kriterium zur Anhang-Filterung stehen Ihnen hierbei

- *'Absender-IP'*
- *'Absender'*
- *'Empfänger'*

zur Verfügung. Sie müssen mindestens eines davon angeben. Als Vorgehensweise haben Sie die Wahl zwischen

- *'annehmen' / 'accept'*
- 'zurückweisen' / 'reject'

Der angegebene Filter wird auf alle Anhänge angewandt, auf welche die *'Liste der Dateiendungen'* zutrifft. Geben Sie mehrere Endungen von Dateianhängen an, so müssen diese durch Kommata getrennt werden (Bsp.: '.exe,.bat'). Sie sollten an dieser Stelle auch den Punkt (.) vor der Dateiendung angeben, da sonst auch ungewollt andere Anhänge entfernt werden könnten. Wenn Sie beispielsweise die Dateiendung „ml“ eintragen, sind hier auch Anhänge mit der Endung „.html“ betroffen. Sollte Sie jedoch als Dateiendungen „.htm“ angeben, sind E-Mailanhänge mit der Endung „.html“ nicht betroffen.

> Beachten Sie, dass Sie entweder einzelne Anhänge freischalten (*'annehmen'*) *oder* entfernen (*'zurückweisen'*). Erzeugen Sie Einträge mit der Regel *'annehmen'*, werden alle anderen Anhänge entfernt. Sollten Sie Einträge mit der Regel *'ablehnen'* erzeugen, werden alle anderen Anhänge durchgelassen.

Beispiele

Nur .pdf-Anhänge einer Absende-Domain komplett freischalten

IP-Adresse des Absenders	leer
Absender E-Mail oder @domain	@domainname
Empfänger E-Mail oder @domain	leer
Vorgehen	*'annehmen' / 'accept'*
Erweiterungen	.pdf

Mails mit .bat- und .exe-Dateianhängen an eine Domain sperren

IP-Adresse des Absenders	eintragen
Absender E-Mail oder @domain	leer
Empfänger E-Mail oder @domain	@domainname
Vorgehen	*'zurückweisen' / 'reject'*
Erweiterungen	.bat,-exe

7.3.8 Domain-Admins

Menüpunkt: *'SPONTS → Tabellen→ Domain-Admins'*

Hier können Sie Administratoren für die im SPONTS eingetragenen lokalen Domains hinzufügen. Ein Domain-Administrator hat alle Berechtigungen eines Administrator in seiner jeweiligen Domain. Er darf Konfigurationen für E-Mail Empfänger, deren Adresse auf diese Domain enden, vornehmen, einschließlich Envelope- und Anhang-Filter.

Domain-Administratoren haben keinen Zugriff auf die Systemeinstellungen des SPONTS oder auf die Liste der Domain-Administratoren.

7.3.9 Proxies

Menüpunkt: *'SPONTS → Tabellen → Proxies'*

Um SPONTS mit mehr als einer Proxy-Einstellung zu nutzen, können sie weitere Konfigurationen an dieser Stelle eintragen. Nach Neueintragungen oder Änderungen in der Liste der Proxies müssen Sie SPONTS neu starten, um diese zu aktivieren.

7.3.10 Benutzer

Menüpunkt: *'SPONTS → Tabellen → Benutzer'*

Um die Authentifizierung von Clients von jeder beliebigen IP-Adresse ohne die aktivierte Prüfung gegen das Backend (Backendcheck aktivieren, S. 48) zu ermöglichen, können Sie hier die Benutzer mit ihren Passworten eintragen.

7.3.11 Statistik

Menüpunkt: *'SPONTS → Tabellen → Statistiken'*

Über die Statistik-Einwilligung können Sie den Versand der täglichen Statistiken über eingehende E-Mails an eine Domain oder einzelne Benutzer kontrollieren. Tragen Sie dazu einzelne E-Mail Adressen oder die entsprechende Domain in die Liste ein.

7.3.12 Virenscanner / E-Mail Desinfektion

Menüpunkt: *'SPONTS → Tabellen → Virenscanner'*

Unter diesem Menüpunkt können Sie die Liste der Benutzer oder Domains bearbeiten, für die eine Desinfektion virenverseuchter E-Mails versucht werden soll, bearbeiten. Zusätzlich muss unter der Konfiguration der Virenscanner die entsprechende Einstellung Infizierte Dateianhänge entfernen(Desinfektion) (S. 52) aktiviert sein.

Die Einwilligungen zur Desinfektion von infizierten E-Mails dürfen aufgrund des Fernmeldegesetzes nur dann für Domänen global eingerichtet werden, wenn Ihre Nutzer einer entsprechenden Betriebsvereinbarung eingewilligt haben, da dies einer Nachrichtenunterdrückung (Zensur) entspricht.

7.4 Aktionen

7.4.1 Backup

Menüpunkt: *'SPONTS → Aktionen → Backup'*

Hier können Sie eine Sicherung der Einstellungen und Datenbanken mit einem Klick auf *'Zip-Archiv'* anfordern. Diese Sicherung enthält die Konfigurationsdatei Ihres

SPONTS, sowie einen vollständigen Auszug der SQL-Tabellen der Datenbanken zum Zeitpunkt der Sicherung.

7.4.2 Neustart

Menüpunkt: *'SPONTS → Aktionen→ Neustart'*

Hier können Sie SPONTS neu starten oder abschalten. Dabei stehen Ihnen die folgenden Möglichkeiten zur Verfügung:

- **SPONTS jetzt neu starten**
  SPONTS-Engine neu starten (schnell)
- **SPONTS aus- und anschalten**
  Warmstart SPONTS inklusive Betriebssystem (langsam)
- **SPONTS abschalten**
  SPONTS herunterfahren (ausschalten).

> Achtung: SPONTS schaltet sich mit 'Shutdown' komplett ab! Einschalten können Sie SPONTS allerdings nur am Gerät selbst.

7.4.3 Cache löschen

Menüpunkt: *'SPONTS → Aktionen→ Cache löschen'*

Es wird der komplette Cache gelöscht. Dieser enthält:

- Hosts, in Verbindung mit der Timing-Analyse (vgl. iKu-Timing-Whitelist aktivieren, S.40)
- durch den SenderDomainCheck geprüfte gültige Domains (vgl. Überprüfung der Absender-Domain, S.66)
- durch den SenderSMTPCheck geprüfte gültige Absender (vgl. Sender Policy Framework, S.67)

7.4.4 SQL

Über den Menüpunkt SQL gelangen sie zu einer Eingabemaske, über die Sie eine Datei mit SQL-Befehlen angeben können, um diese auf der Datenbank auszuführen.

7.5 UCE

7.5.1 UCE-Einstellungen

Der Bereich UCE (Unsolicited Commercial E-Mail - Unerwünschte Werbe-Mail) beinhaltet Einstellungen zur Spam-Abwehr. Die meisten Einstellungen beziehen sich auf Checks und Zensoren. Dies sind einzelne Programmelemente, welche Aspekte einer eingehenden Mail analysieren und bewerten. Hierbei können Sie (Straf-)Punkte und Bewertungsfaktoren für jeden zutreffenden Check vergeben. Überschreitet die erreichte Punktzahl (Score) einstellbare Grenzwerte, so wird gewarnt oder sogar die Annahme der Mail verweigert.

Zusätzlich können Sie bei einigen Modulen angeben, was mit einer E-Mail passieren soll, die - unabhängig von anderen aktivierten Checks - von diesem Check als UCE eingestuft wird. Die durch einzelne Checks gesetzten Regeln zum

weiteren Verfahren mit einer eingehenden Mail können durch nachfolgende Checks lediglich erhöht werden. Sollte die Gesamtpunktzahl aller Checks nicht zu einer UCE-Bewertung einer E-Mail führen, wird trotzdem die höchste zuvor gesetzte Regel genutzt.

Die möglichen Bewertungsregeln in aufsteigender Reihenfolge sind:

- **Warnung**
- **temporäre Ablehnung**
- **permanente Ablehnung**
- **Eintragen in die Auto-Blacklist**

Empfohlene Vorgehensweise für Spam-Abwehr

SPONTS lässt sich so einstellen, dass potenzielle Spam-Nachrichten nur markiert, aber nicht geblockt werden. Sie sollten SPONTS für eine Weile auf diese Weise laufen lassen und über das Journal prüfen, ab welcher Punktzahl ein Blocken sinnvoll ist. Ebenso können Sie erkennen, welche erwünschten Werbemail-Absender - beispielsweise Lieferanten und Newsletter - in die Whitelist eingetragen werden müssen. Erst wenn keine erwünschte Mail eine Punktzahl über einem bestimmten Grenzwert - beispielsweise 5 - mehr erhält, sollten Sie das Blockieren aktivieren.

Die UCE-Einstellungen des SPONTS sind – wie die Systemeinstellungen – unterteilt in statische und dynamische Einstellungen.
Sollten Sie Änderungen an statischen Einstellungen vornehmen, müssen Sie SPONTS neu starten, nachdem Sie die Einstellungen durch '*speichern*' am Ende der Einstellungsseite übernommen haben. Erst dann werden diese wirksam (vgl. 7.4.2 Neustart, S.62).
Sollten Sie Änderungen an dynamischen Einstellungen vornehmen, werden diese wirksam, sobald Sie die Einstellungen durch '*speichern*' am Ende der Einstellungsseite übernommen haben.

Begriffe der UCE-Einstellungen

Die UCE-Einstellungen beinhalten für die Zensoren, sowie die gesamte UCE-Bewertung Einstellungspunkte mit übereinstimmenden Bezeichnungen, welche an dieser Stelle erklärt werden.

- **Zensor-Punktzahl**
  Bei einigen Checks oder Zensoren können Sie festlegen, welche Punktzahl als Ergebnis bei Zutreffen des Checks als Ergebnis genutzt werden soll.
- **Bewertungsfaktoren für Zensor-Ergebnis**
  Das Ergebnis eines Checks oder Zensors wird mit dem angegebenen Bewertungsfaktoren multipliziert. Durch diese Einstellung können Sie einzelne Zensoren mit ihren Ergebnissen stärker in die Gesamtwertung einfließen lassen.

Hinweis: Sollte ein Bewertungsfaktor von '0' konfiguriert sein, wird der entsprechende Zensor – trotz seiner Aktivierung – nicht zu einer Bewertung einer E-Mail beitragen.

- **Zensor-Ergebnis**
  Das Zensor-Ergebnis ergibt sich aus dem Produkt der Zensor-Punktzahl und dem Bewertungsfaktor für das Zensor-Ergebnis.

```
'Zensor-Ergebnis' =
'Zensor-Punktzahl' * 'Bewertungsfaktor für Zensor-Ergebnis'
```

- **Gesamtbewertung einer E-Mail**
  Die Gesamtbewertung einer E-Mail ist die Summe der Zensor-Ergebnisse aller aktivierten Zensoren
- **Punktzahl, die zu einer Warnung führt**
  An diesen Stellen können Sie die Punktzahl eines einzelnen Zensors oder der gesamten UCE-Erkennung angeben, ab der eine E-Mail mit einer Header-Zeile `'X-SPONTS-Warning'` versehen werden soll.

Geben Sie an diesen Stellen den Wert des Zensor-Ergebnisses an, wenn z.B. immer eine Warnung erzeugt werden soll, sobald ein Zensor greift.

Geben Sie an diesen Stellen den Wert '`9999`' an, wenn dieses Ergebnis niemals erreicht werden soll.

- **Punktzahl, die zu einer temporären Ablehnung führt**
  An diesen Stellen können Sie die Punktzahl eines einzelnen Zensors oder der gesamten UCE-Erkennung angeben, ab der eine E-Mail temporär abgelehnt werden soll. Der Absender erhält auf SMTP-Ebene eine Meldung, dass die entsprechende Mailbox zeitweise nicht verfügbar ist.
- **Punktzahl, die zu einer permanenten Ablehnung führt**
  An diesen Stellen können Sie die Punktzahl eines einzelnen Zensors oder der gesamten UCE-Erkennung angeben, ab der eine E-Mail permanent abgelehnt werden soll. Der Absender erhält eine SMTP-Ebene eine Meldung, dass die entsprechende Mailbox permanent nicht verfügbar ist.
- **Punktzahl, die zu einer Eintragung in die Auto-Blacklist führt**
  An diesen Stellen können Sie die Punktzahl eines einzelnen Zensors oder gesamten UCE-Erkennung angeben, ab der eine E-Mail permanent abgelehnt und zusätzlich die Kombination aus Absenderadresse und sendendem Mailserver in die Automatische Schwarze Liste eingetragen wird (vgl. 7.5.2 Auto-Blacklist, S.73).
  Über diese Liste können UCE-Mails geblockt werden, ohne die UCE-Zensoren zu durchlaufen. Die Nutzung der Schwarzen Liste kann Systemressourcen des SPONTS schonen.

Statische Einstellungen: Allgemein

Menüpunkt: *'UCE'*

Bei Änderungen der statischen Einstellungen zu UCE muss SPONTS – wie auch bei statischen Systemeinstellungen – neu gestartet werden, damit diese wirksam werden.

- **Realtime Blacklists (RBLs) aktivieren**
  Aktiviert die Nutzung des RBL-Zensors (vgl. 7.5.1 Realtime Blacklists, S.65).
  Voreinstellung: `aktiviert`

- **Domain-Überprüfung des Absenders aktivieren**
  Aktiviert die Überprüfung der Absender-Domain (vgl. 7.5.1 Überprüfung der Absender-Domain, S.66).
  Voreinstellung: `aktiviert`
- **SPF-Überprüfung aktivieren**
  Aktiviert SPF-Checks des Absenders (vgl. 7.5.1 Sender Policy Framework, S.67).
  Voreinstellung: `aktiviert`
- **SMTP-Überprüfung des Absenders aktivieren**
  Aktiviert die Überprüfung des Absenders über SMTP (vgl. 7.5.1 SMTP-Überprüfung des Absenders, S.68).
  Voreinstellung: `aktiviert`
- **Zensor für RFC-Konformität aktivieren**
  Aktiviert die Prüfung eingehender E-Mails auf RFC-Konformität (vgl. 7.5.1 Zensor für RFC-Konformität, S.68).
  Voreinstellung: `aktiviert`
- **URL-Blacklists (URIDNSBLs) aktivieren**
  Aktiviert den URIDNS-Zensor, der überprüft, ob der Inhalt ("body") einer Mail URLs enthält, die in einer Schwarzen Liste (URIDNS blacklist) stehen.
  Voreinstellung: `aktiviert`
- **Zensor Spamassassin aktivieren**
  Aktiviert den Zensor Spamassassin zur Inhaltsüberprüfung einer eingehenden E-Mail (vgl. 7.5.1 Spamassassin, S.70).
  Voreinstellung: `aktiviert`
- **Höchstalter von Auto-Blacklist-Einträgen (Sek.)**
  Maximales Alter der Einträge der Automatischen Schwarzen Liste. Haben Einträge in dieser Liste dieses Alter erreicht, werden sie vom Cron-Dienst aus der Liste entfernt (vgl. 7.5.2 Auto-Blacklist, S.73).
  Voreinstellung: `1209600` (14 Tage)

Realtime Blacklists (RBLs)

Die Einstellungen des RBL-Checks sind Laufzeit-Einstellungen. Nach Änderungen an diesen Einstellungen muss SPONTS nicht neu gestartet werden, sie greifen sofort.

Dieser Check prüft, ob der versendende Server einer eingehenden E-Mail auf einer öffentlichen Schwarzen Liste vermerkt wurde. Fundstellen in den einzelnen angegebenen Listen ergeben Punktzahlen, die in ihrer Summe das Checkergebnis ergeben. Das so errechnete Ergebnis wird mit dem zu diesem Check angegebenen Bewertungsfaktor multipliziert und geht in die Gesamtbewertung einer E-Mail ein.

- **RBL-Server (Liste)**
  Komma getrennte Liste von RBL-Servern. Jede Fundstelle ergibt einen Bewertungspunkt. Abweichende Bewertungen können in eckigen Klammern hinter dem RBL-Server angegeben wird, z.B.
  '`list.dsbl.org[1.25],relays.ordb.org`'.
  Voreinstellung: `list.dsbl.org,relays.ordb.org`
- **Bewertungsfaktor für Zensor-Ergebnis**
  Voreinstellung: `3`

- **Punktzahl, die zu einer Warnung führt**
  Voreinstellung: `9999`
- **Punktzahl, die zu einer temporären Ablehnung führt**
  Voreinstellung: `1`
- **Punktzahl, die zu einer permanenten Ablehnung führt**
  Voreinstellung: `9999`
- **Punktzahl, die zu einem Eintrag in die Auto-Blacklist führt**
  Voreinstellung: `9999`

Überprüfung der Absender-Domain (DNS)

Die Einstellungen der Überprüfung der Absender-Domain Laufzeit-Einstellungen. Nach Änderungen an diesen Einstellungen muss SPONTS nicht neu gestartet werden, sie greifen sofort.

Dieser Check überprüft, ob die angegebene Absender-Domain existiert. Um Schleifen zu verhindern, wird dies erst gemacht, sobald der Sende-Server den Nachrichtentext schicken will. Sollten Informationen zur ermittelten Absender-Domain nicht existent sein, wird das jeweilige Zensor-Ergebnis mit dem eingestellten Bewertungsfaktor multipliziert und geht in die Gesamtbewertung einer E-Mail ein. Die Überprüfung ist riskant, da einige Domains keine MX-(MailExchange-) Server haben, z.B. Mailinglisten-Server. Die Bewertungen dieses Checks sollten aus diesem Grund nicht zu hoch eingestellt werden.

- **Bewertungsfaktor für Zensor-Ergebnis**
  Bewertungsmultiplikator für Domains ohne DNS-Einträge vom Typ MX oder A.
  Voreinstellung: `1`
- **Punktzahl für 'kein MX'**
  Bewertung für Domains ohne MX-Eintrag, für die jedoch eine IP-Adresse (A-Eintrag) ermitteln werden können.
  Voreinstellung: `0,25`
- **Punktzahl für 'kein MX, keine IP'**
  Bewertung für eine Domain ohne MX-Eintrag und ohne IP-Adresse (A-Eintrag).
  Voreinstellung: `1`
- **Punktzahl bei ungültiger Domain**
  Bewertung für ungültige oder unbekannte Domains.
  Voreinstellung: `2`
- **Punktzahl, die zu einer Warnung führt**
  Voreinstellung: `9999`
- **Punktzahl, die zu einer temporären Ablehnung führt**
  Voreinstellung: `1`
- **Punktzahl, die zu einer permanenten Ablehnung führt**
  Voreinstellung: `9999`
- **Punktzahl, die zu einem Eintrag in die Auto-Blacklist führt**
  Voreinstellung: `9999`

Sender Policy Framework (SPF)

Die Einstellungen zum Sender Policy Framework sind Laufzeit-Einstellungen. Nach Änderungen an diesen Einstellungen muss SPONTS nicht neu gestartet werden, sie greifen sofort.

Das Sender Policy Framework ist eine Erweiterung des DNS-Eintrags von Domains, in deren TXT-Einträgen angegeben werden wird, welche Server im Namen dieser Domain E-Mails versenden dürfen. Nähere Informationen zu SPF und der Konfiguration Ihres DNS-Eintrags finden Sie unter http://spf.pobox.com/.

> Häufig werden E-Mails, welche über einen Backup-MX empfangen werden durch den SPF-Check geblockt, da dieser nicht im SPF-Eintrag der entsprechenden Domain vermerkt ist.
> Tragen Sie in diesen Fällen den Backup-MX mit seiner IP-Adresse in die Tabelle Envelope (S. 58) mit der Regel 'niemals zurückweisen / never-reject' ein.

- **Bewertungsfaktor für Zensor-Ergebnis**
  Bewertungsmultiplikator für E-Mails, die von einem Server kommen, dessen SPF-Überprüfung negativ ausgefallen ist.
  Voreinstellung: `3`
- **Punktzahl, die zu einer Warnung führt**
  Voreinstellung: `1`
- **Punktzahl, die zu einer temporären Ablehnung führt**
  Voreinstellung: `2`
- **Punktzahl, die zu einer permanenten Ablehnung führt**
  Voreinstellung: `3`
- **Punktzahl, die zu einem Eintrag in die Auto-Blacklist führt**
  Voreinstellung: `9999`
- **Punktzahl für das SPF-Ergebnis NONE**
  Bewertung für Server, deren Domain keinen veröffentlichten SPF-Eintrag haben. Server ohne zugehörigen SPF-Eintrag sollten nicht abgewiesen werden.
  Voreinstellung: `0`
- **Punktzahl für das SPF-Ergebnis NEUTRAL**
  Bewertung für Server, deren Domain keinen aussagekräftigen SPF-Eintrag veröffentlichen. Ein solcher neutraler SPF-Eintrag muss wie ein fehlender Eintrag behandelt werden.
  Voreinstellung: `0`
- **Punktzahl für das SPF-Ergebnis FAIL**
  Bewertung für Server mit einem negativen SPF-Eintrag. Solche Server gehören laut SPF-Eintrag der angebenden Domain nicht zur Gruppe der zulässigen Mailserver und dürfen keine E-Mails im Namen der Domain verschicken.
  Voreinstellung: `3`
- **Punktzahl für das SPF-Ergebnis TEMP_ERROR**
  Bewertung für Server, deren SPF-Überprüfung einen vorübergehenden Fehler während DNS-Abfrage oder anderen Verarbeitungsschritten des Zensors ergeben haben.
  Voreinstellung: `0`

- **Punktzahl für das SPF-Ergebnis PERM_ERROR**
  Bewertung für Server, deren SPF-Überprüfung zu einem behebbaren Fehler geführt haben, z.B. bei Fehlern im SPF-Eintragsformat.
  Voreinstellung: `1`

SMTP-Überprüfung des Absenders

Die Einstellungen zur SMTP-Überprüfung des Absenders sind Laufzeit-Einstellungen. Nach Änderungen an diesen Einstellungen muss SPONTS nicht neu gestartet werden, sie greifen sofort.

Dieser Check überprüfen, ob der angegebene Absender einer E-Mail überhaupt existiert. Dazu wird eine SMTP-Verbindung zum Absende-Server öffnet und versucht, eine Mail an den Absender zu schicken. Dies wird auch 'Call-Out' genannt.

- **Bewertungsfaktor für Zensorergebnis**
  Bewertungsfaktor für E-Mails, deren Absender keine E-Mail vom Empfänger annehmen.
  Voreinstellung: `1`
- **Punktzahl, die zu einer Warnung führt**
  Voreinstellung: `9999`
- **Punktzahl, die zu einer temporären Ablehnung führt**
  Voreinstellung: `1`
- **Punktzahl, die zu einer permanenten Ablehnung führt**
  Voreinstellung: `9999`
- **Punktzahl, die zu einem Eintrag in die Auto-Blacklist führt**
  Voreinstellung: `9999`
- **Punktzahl für temporäre SMTP-Ergebnisse (4xx)**
  Punktzahl, welche vom Zensor vergeben wird, sobald der Absender vorübergehend keine E-Mails vom Empfänger annimmt (SMTP 4xx). Gründe dafür können z.B. Greylisting, oder überfüllte Mailaccounts sein.
  Voreinstellung: `0,5`
- **Punktzahl für permanente SMTP-Ergebnisse (5xx)**
  Punktzahl, welche vom Zensor vergeben wird, sobald der Absender dauerhaft keine E-Mails vom Empfänger annimmt (SMTP 5xx). Gründe dafür können z.B. ungültige Absenderadressen, Blacklisting, aber auch ein kurzzeitiger Ausfall des Mailservers sein.
  Voreinstellung: `1`

Zensor für RFC-Konformität

Die Einstellungen des Zensors für RFC-Konformität sind Laufzeit-Einstellungen. Nach Änderungen an diesen Einstellungen muss SPONTS nicht neu gestartet werden, sie greifen sofort.

Dieser Zensor überprüft die Einhaltung von RFC 821 und 822 in Bezug auf Absender- und Empfänger-Adressen. Einige Spammer und leider auch einige legitime Mailserver halten sich nicht an den RFC und verschicken fehlerhafte Nachrichten. Deshalb sollten Sie hierfür Punkte vergeben, aber nicht blockieren.

- **Bewertungsfaktor für Zensorergebnis**
  Bewertungsfaktor für eine erkannte RFC-Missachtung.
  Voreinstellung: `2`
- **Vorgehensweise**
  Vorgehensweise für E-Mails, die nicht den RFC-Standards 821 und 822 entsprechen. An dieser Stelle 'permanente Ablehnung' oder 'Automatische Blacklist' einzustellen ist nicht ratsam, da es zu viele defekte Mailserver gibt.
  Voreinstellung: `nichts`
  Mögliche Vorgehensweisen sind:
  - **nichts**
    Trotz einer Missachtung der RFCs soll dieser Zensor von sich aus keine Vorgehensweise über die entsprechende E-Mail erwirken.
  - **Benutzer warnen**
    Dieser Zensor soll bei einer Missachtung der RFC eine Warnung des Empfängers erwirken.
  - **temporäre Ablehnung**
    Dieser Zensor soll eine temporäre Ablehnung der E-Mail erwirken.
  - **permanente Ablehnung**
    Dieser Zensor soll eine permanente Ablehnung der E-Mail erwirken.
  - **Automatische Blacklist**
    Dieser Zensor soll bei einer Missachtung der RFC die Kombination aus versendendem Server und Absender in die Automatische Schwarze Liste eintragen.

URL-Blacklist (URIDNSBL)

Die Einstellungen des URIDNSBL-Checks sind Laufzeit-Einstellungen. Nach Änderungen an diesen Einstellungen muss SPONTS nicht neu gestartet werden, sie greifen sofort.

Dieser Zensor überprüft, ob eine E-Mail Links auf http-Adressen enthält, welche in einem einer öffentlichen Schwarzen Liste vermerkt wurden.

- **Bewertungsfaktor für Zensorergebnis.**
  Voreinstellung: `1`
- **URIDNSBL-Server (Liste)**
  Komma getrennte Liste von URIDNSBL-Servern. Jede Fundstelle ergibt einen Bewertungspunkt.
  Voreinstellung: `multi.surbl.org`
- **Vorgehensweise**
  Vorgehensweise für E-Mails, die nicht den RFC-Standards 821 und 822 entsprechen. An dieser Stelle 'permanente Ablehnung' oder 'Automatische Blacklist' einzustellen ist nicht ratsam, da es zu viele defekte Mailserver gibt.
  Voreinstellung: `permanente Ablehnung`
  Mögliche Vorgehensweisen sind:
  - **nichts**
    Trotz einer Missachtung der RFCs soll dieser Zensor von sich aus keine Vorgehensweise über die entsprechende E-Mail erwirken.

- **Benutzer warnen**
  Dieser Zensor soll bei einer Missachtung der RFC eine Warnung des Empfängers erwirken.
- **temporäre Ablehnung**
  Dieser Zensor soll eine temporäre Ablehnung der E-Mail erwirken.
- **permanente Ablehnung**
  Dieser Zensor soll eine permanente Ablehnung der E-Mail erwirken.
- **Automatische Blacklist**
  Dieser Zensor soll bei einer Missachtung der RFC die Kombination aus versendendem Server und Absender in die Automatische Schwarze Liste eintragen.

Greylisting

Greylisting ist defaultmäßig **deaktiviert**, weil es prinzipbedingt jedes Mal zu einer erheblichen Verzögerung führt, wenn man zum ersten Mal Email von einem Sender erhält. Die SPONTS Timing-Analyse erzielt bereits eine sehr guten Spammer-Erkennungsrate. Die Vor- und Nachteile von Greylisting sollten insofern sorgfaltig abgewogen werden.

Greylisting bewirkt, dass bisher unbekannte Kombinationen von Sender-IP-Adresse, Absender und Empfänger in eine sog. 'Greylist' eingetragen werden. Solange sich ein Eintrag in der Greylist befindet, werden entsprechende Emails abgewiesen (mit 'Temporary Failure').

Ein Eintrag wird nur dann aus der Greylist entfernt (und in die Whitelist verschoben), wenn nach Ablauf einer Mindestzeit und vor Ablauf einer Maximalzeit erneut eine Email mit der gleichen Kombination von Sender-IP, Absender und Empfänger eingeht.

Wird die Maximalzeit überschritten, dann wird das Alter des Greylisting-Eintrags auf 0 zurück gesetzt, d.h. die Wartezeit beginnt von vorn.

- **Initial greylisting delay**
  Mindest-Verweildauer (in Sekunden) für Einträge in der Greylist
- **Höchstalter von unbestätigten Einträgen (Sek.)**
  Maximalalter von Greylist-Einträgen

Zensor Spamassassin

Die Einstellungen des Zensors Spamassassin sind Laufzeit-Einstellungen. Nach Änderungen an diesen Einstellungen muss SPONTS nicht neu gestartet werden, sie greifen sofort.

Spamassassin (http://www.spamassassin.org/) ist ein heuristischer Spam-Erkenner, der mit fast 1.000 verschiedenen Tests erkennt, ob es sich bei einer Nachricht um Spam handelt oder nicht. Hierbei wird eine Punktzahl anhand des E-Mail Inhalts vergeben, die umso höher ist, je wahrscheinlicher es ist, dass es sich bei der Nachricht um Spam handelt.

- **Bewertungsfaktor für Zensor-Ergebnis**
  Bewertungsmultiplikator für die Ergebnisse von Spamassassin.
  Voreinstellung: `1`

- **Punktzahl, die zu einer Warnung führt**
  Voreinstellung: `9999`
- **Punktzahl, die zu einer temporären Ablehnung führt**
  Voreinstellung: `9999`
- **Punktzahl, die zu einer permanenten Ablehnung führt**
  Voreinstellung: `9999`
- **Punktzahl, die zu einem Eintrag in die Auto-Blacklist führt**
  Voreinstellung: `9999`
- **Servername von spamd**
  Name des Servers, auf dem 'spamd', der daemon (Hintergrundprozess) von SpamAssassin läuft.
  Voreinstellung: `localhost`
- **IP-Portnummer von spamd**
  Port, über den 'spamd' erreicht wird.
  Voreinstellung: 783
- **Max. Anzahl an Spamassassin-Instanzen**
  Maximale Anzahl der gleichzeitig laufenden Spamassassin-Instanzen.
  Voreinstellung: `2`
- **Wartezeit auf verfügbaren Spamassassin (Sek.)**
  Wenn die maximale Anzahl an parallel laufenden Spamassassin-Instanzen erreicht ist, wird diese Zeit an Sekunden auf das Freiwerden einer Instanz gewartet, bevor die Verbindung getrennt wird.
  Voreinstellung: `240` (4 Minuten)
- **maximale E-Mail-Größe**
  Maximale Größe der E-Mails in Bytes, welche durch SpamAssassin überprüft werden sollen. Dies spart Rechenleistung, da Spammer in der Regel kleine Nachrichten erzeugen, um in kurzer Zeit viele Nachrichten verschicken zu können.
  Voreinstellung: `100000`
- **Ergebnisbericht**
  Spamassassin-Ergebnisse, welche in die System-Logdatei geschrieben werden sollen.
  Voreinstellung: `alle`
  Als Arten des Ergebnisberichts stehen folgende Einstellungen zur Verfügung:
  - **keine**
    keine Berichte
  - **nur Spam**
    nur Berichte über Spam-Mails
  - **alle**
    Berichte über alle E-Mails

Inhaltsanalyse

Für diese Inhaltsanalyse wird von eingehenden Emails jeweils eine sogenannte „weiche Prüfsumme“ erzeugt und mit einem Server von iKu abgeglichen, der eine aktuelle schwarze Liste von Prüfsummen typischer Spam-Mails verwaltet.

- **Bewertungsfaktor für Zensor-Ergebnis**
  Bewertungsmultiplikator für E-Mails, die von der Inhaltsanalyse als auf der schwarzen Liste stehend erkannt wurden
  Voreinstellung: `1`
- **Vorgehensweise**
  Vorgehensweise für E-Mails, die von der Inhaltsanalyse als auf der schwarzen Liste stehend erkannt wurden.
  Voreinstellung: `permanente Ablehnung`

UCE-Punktzahl-Auswertung

Die Einstellungen der UCE-Punktzahl-Auswertung sind Laufzeit-Einstellungen. Nach Änderungen an diesen Einstellungen muss SPONTS nicht neu gestartet werden, sie greifen sofort.

Hier geben Sie an, was anhand der durch alle aktivierten UCE-Checks berechneten Gesamtbewertung einer E-Mail mit dieser geschehen soll.

- **Punktzahl, die zu einer Warnung führt**
  Voreinstellung: `4`
- **Punktzahl, die zu einer temporären Ablehnung führt**
  Voreinstellung: `9999`
- **Punktzahl, die zu einer permanenten Ablehnung führt**
  Voreinstellung: `9999`
- **Punktzahl, die zu einem Eintrag in die Auto-Blacklist führt**
  Voreinstellung: `9999`
- **Warnung in Betreffzeile einfügen**
  Wenn eine E-Mail die für Warnungen definierte Mindestspambewertung erreicht, die Betreffzeile der Mail mit einem Präfix versehen. Diese Einstellung können Sie nutzen, um die mit einer Warnung versehenen E-Mails in Ihrem E-Mail Programm durch Filter in spezielle Ordner sortieren zu lassen und die Empfänger auf eine mögliche Spam-E-Mail aufmerksam zu machen.
  Voreinstellung: `aktiviert`
- **Text der Warnung**
  Präfix, welcher bei einer als Spam erkannten Mail am Beginn der Betreffzeile angefügt wird.
  Voreinstellung: `{{SPAM}}`

Proaktive Anti-UCE Maßnahmen

Die Einstellungen der Proaktiven Anti-UCE-Maßnahmen sind Laufzeit-Einstellungen. Nach Änderungen an diesen Einstellungen muss SPONTS nicht neu gestartet werden, sie greifen sofort.

Für eingehende E-Mails, welche über die Envelope-Filterung mit der Vorgehensweise 'Spamfalle' gefiltert wurden (vgl. 7.3.6 Envelope, S.58) können Sie hier die Einstellungen der Spamfalle vornehmen. Eine Spamfalle blockiert den versendenden Server eine bestimmte Zeit und senkt so dessen Maildurchsatz und wird aus diesem Grund auch als Teergrube bezeichnet. Der Einsatz von Spamfallen sollte nur für Server oder Adressen genutzt werden, bei denen Sie sicher sind, dass sie der Verbreitung von Spam dienen.

- **Meldung, die eine Teergrube beim Verzögern sendet**
  SMTP-Meldung, welche von der Teergrube beim Verzögern des E-Mail Empfang gesendet wird.
  Voreinstellung: `please hold the line`
- **Gesamt-Verzögerung der Teergrube (Sek.)**
  Voreinstellung: `60`

Sonstige Einstellungen

Ein besonderes Feature von SPONTS/UCE ist die Möglichkeit, Emails zwar auf SMTP-Ebene mit einer Fehlermeldung als nicht zugestellt zu quittieren, sie aber trotzdem zuzustellen:

- **Geblockte Mails zustellen**
  Hiermit aktivieren/deaktivieren Sie die Zustellung von Emails, die auf SMTP-Ebene abgelehnt wurden.

> Bedenken Sie, dass für der sendende Mailserver eine von SPONTS abgelehnte Email als nicht zugestellt bzw. nicht zustellbar betrachten wird und dem Absender dies höchstwahrscheinlich in Form einer entsprechenden Fehlermeldungs-Email mitteilt. Die Option 'Geblockte Mails zustellen' sollte deswegen mit Vorsicht verwendet werden.

7.5.2 Auto-Blacklist

Menüpunkt: '*SPONTS → UCE → Auto-Blacklist*'

Die Automatische Blacklist wird von SPONTS selbständig ergänzt, sobald die Punktzahl einer Nachricht den entsprechenden Grenzwert übersteigt. Gesperrt wird die Kombination von Absendeserver-IP und Absender, um bei gefälschten Absendern keine Störungen des regulären Mailbetriebs zu verursachen. Die Tabelle enthält eine Spalte '*hits*', die die Anzahl der Treffer angibt. Die Einträge werden nach einem einstellbaren Zeitraum automatisch gelöscht.

> Sollte eine Mail fälschlicherweise eine viel zu hohe Punktzahl erhalten haben, so müssen Sie den Absender aus dieser Liste entfernen, damit er wieder Mails an Sie schicken kann.

7.5.3 UCE Opt-In / UCE-Einwilligung

Menüpunkt: '*UCE → UCE Opt-in*'

Die Liste der UCE-Einwilligungen beinhaltet alle Empfängeradressen und Domains, für welche die UCE-Prüfungen genutzt werden sollen. Für Adressen oder Domains, die nicht in dieser Liste eingetragen sind, werden keine UCE-Prüfungen vorgenommen.

Die Einwilligungen für UCE dürfen aufgrund des Fernmeldegesetzes nur dann für Domänen global eingerichtet werden, wenn Ihre Nutzer einer entsprechenden Betriebsvereinbarung eingewilligt haben, da dies einer Nachrichtenunterdrückung (, Zensur) entspricht.

7.5.4 Einweg- / Wegwerfadressen

Unter Einweg- bzw. Wegwerfadressen verstehen sich E-Mail Adressen zur kurzzeitigen Nutzung. Diese können z.B zur Anmeldung auf Webseiten genutzt

werden, wobei eine Einwegadresse im Format `[schlüsselwort].[anzahl].[empfänger]`
oder
`[schlüsselwort].[empfänger]` angegeben werden kann.
Benutzer, die sich zur Nutzung der Einwegadressen angemeldet haben, müssen die selbst erzeugten Adressen nicht im SPONTS angeben. Eine neue Einwegadresse wird vom System übernommen und die mit dieser Adresse angegebene Anzahl von E-Mails wird an den eigentlichen Empfänger weitergeleitet.

> **Beispiel:**
> einwegadresse.12.benuter@domain.de
>
> E-Mails an diese Adresse werden an den Empfänger <benutzer@domain.de> weitergeleitet. Nach 12 empfangenen E-Mails wird diese Adresse blockiert.

Die Anzahl der über eine Einwegadresse empfangenen E-Mails, sowie die noch verfügbare Anzahl von E-Mails, bevor der Empfang blockiert wird, ist über die Liste der Adressen und Empfänger einsehbar und konfigurierbar.

Einstellungen zu Einwegadressen

Menüpunkt: *'UCE → Einwegadressen'*

- **Einwegadressen erlauben**
  Erlaubt die Nutzung von Einwegadressen. Eine Einwilligung (Opt in) für Einwegadressen muss für die entsprechenden E-Mail Adressen oder Domains angegeben werden. Diese Einstellung wird mit Klick auf 'speichern' übernommen.
  Voreinstellung: `deaktiviert`
- **automatische Maximalzahl**
  Begrenzung der Maximalzahl für automatisch generierte Einwegadressen. Sollte ein Benutzer in einer Einwegadresse eine größere Zahl empfangbarer E-Mails angegeben haben, wird diese auf die Maximalzahl gesetzt.
  Voreinstellung: `20`

Einwegadresse und Empfänger

Menüpunkt: *'UCE → Einwegadressen → Adressen und Empfänger'*

Diese Liste enthält die bisher angenommenen Einwegadressen und ihre Empfänger mit Statistiken. Die Statistiken der Einwegadressen enthalten:

- **Schlüsselwort**
  Das mit einer Einwegadresse angegebene Schlüsselwort.
- **Empfängeradresse**
  Eigentliche Empfängeradresse einer Einwegadresse.
- **max. E-Mails**
  Die mit der Angabe einer Einwegadresse erzeugte Maximalzahl erlaubter Einwegadressen, bzw. die eingestellte automatische Maximalzahl.
- **verfügbare E-Mails**
  Anzahl der über diese Einwegadresse noch akzeptierten E-Mail. Diese Zahl wird mit jeder weitergeleiteten E-Mail gesenkt, sobald der Wert 0 erreicht ist, werden alle weiteren E-Mails geblockt. Diese Zahl kann über den Link

'bearbeiten' der entsprechenden Schlüsselwort/E-Mail Kombination verändert werden, um mehr als die ursprüngliche Anzahl an E-Mails zu erlauben.

- **weitergeleitete E-Mails**
  Gesamtzahl der bisher weitergeleiteten E-Mails. Diese Zahl kann größer sein, als die ursprüngliche Maximalzahl einer Einwegadresse, da die Zahl der noch verfügbaren E-Mails korrigiert werden kann.
- **geblockte E-Mails**
  Gesamtzahl der geblockten E-Mails einer Einwegadresse.

Über den Link 'bearbeiten' können Sie Einstellungen an einer Einwegadresse vornehmen, über den Link 'löschen' können Sie eine registrierte Einwegadresse löschen.

Einwilligung zu Einwegadressen

Menüpunkt: *'UCE → Einwegadressen → Opt-in'*

Liste der Empfängeradressen und -domains, für die der Empfang von Einwegadressen erlaubt ist. Empfänger und Domains, welche nicht in dieser Liste eingetragen sind, können keine Einwegadressen empfangen.

7.6 UMS

7.6.1 UMS verwenden

> UMS erlaubt den Zugriff auf die Warteschlange per POP3. Der UMS-Administrator kann auf alle Emails zugreifen. Benutzern kann der Zugriff auf Emails erlaubt werden, die an sie gerichtet sind.

Alle eingehenden E-Mails werden zuerst in einer Warteschlange gespeichert. Aus dieser Warteschlange werden die Nachrichten an das Backend geschickt. Ist das Backend nicht erreichbar, so verbleiben sie in der Warteschlange, bis das Backend wieder erreichbar ist. Hierbei wird in regelmäßigen Abständen geprüft, ob das Backend erreichbar ist. Während der Ausfallzeit kann der Administrator per POP3 auf diese Warteschlange zugreifen.

> Das Löschen einer Nachricht entfernt diese endgültig aus der Warteschlange. Deshalb muss in Ihrem Mail-Programm beim POP3-Abruf die Option „Nachrichten auf dem Server belassen“ aktiviert sein.

SPONTS/UMS unterstützt UIDL, so dass jede Nachricht nur einmal heruntergeladen wird.

7.6.2 Einstellungen

Menüpunkt: *'UCE'*

Die Einstellungen zu UMS sind unterteilt in statische und dynamische Einstellungen. Änderungen an statischen Einstellungen werden erst nach einem Neustart des SPONTS wirksam, Änderungen an dynamischen Einstellungen werden sofort wirksam.

> Sie sollten unbedingt SSL verschlüsseltes POP3 (POP3/S) verwenden, da sonst die Passwörter und der Nachrichtentext unverschlüsselt übermittelt werden.

- **POP3-Bind-Adresse**
  IP-Adresse, auf der der POP3-Dienste laufen soll. Normalerweise können Sie dieses Feld leer lassen, der Dienst läuft dann auf allen IP-Adressen des SPONTS.
  Voreinstellung: 127.0.0.1
- **POP3-Portnummer**
  Port-Nummer für den POP3 Dienst. Beachten Sie, dass der hier voreingestellte Port (11110) nicht der Standardport für POP3 ist. Sie müssen diesen Port auch auf dem E-Mail Client einstellen, den Sie für den UMS-Zugang nutzen. Um den POP3 Dienst zu deaktivieren, geben Sie 0 als Port an.
  Voreinstellung: 11110
- **POP3/S-Portnummer**
  Port-Nummer für den POP3 Dienst über SSL. Beachten Sie, dass der hier voreingestellte Port (11995) nicht der Standardport für POP3/S ist. Sie müssen diesen Port auch auf dem E-Mail Client einstellen, den Sie für den UMS-Zugang nutzen.
  Voreinstellung: 11995
- **Gültige Server und Netzwerke von POP3-MUAs**
  Netze, aus denen der POP3-Dienst genutzt werden darf (zur Eingabe-Syntax siehe IP-Adressen und Netzwerke, Seite 37).
  Die Angabe des Netzes 0.0.0.0/0.0.0.0 erlaubt alle Hosts, die diesen Rechner erreichen, sollte aber aus Sicherheitsgründen unbedingt vermieden werden.
  Voreinstellung: `127.0.0.1`
- **POP3-Timeout (Sek.)**
  Wartezeit in Sekunden, nach der eine inaktive Verbindung abgebrochen wird.
  Voreinstellung: 900 (15 Minuten)
- **POP3 admin username**
  Benutzername für UMS-Zugang
- **POP3 admin password**
  Passwort für UMS-Zugang
- **Allow POP3 access by users**
  Wenn diese Option eingeschaltet ist, können alle Benutzer, deren Email-Adresse in der Tabelle 'Benutzer' eingetragen ist, per POP3 auf Emails zugreifen, die an ihre Adresse gerichtet ist. Das zu verwendende Passwort ergibt sich aus der Tabelle 'Benutzer'.

7.6.3 Konfiguration des Zugriffs

In der SPONTS-Web-GUI können Sie alle Einstellungen für UMS vornehmen. Um zugreifen zu können, müssen Sie den zugreifenden Host als 'Gültige Server und Netzwerke von POP3-MUAs' eintragen. Hier können Sie einzelne IP-Adressen oder komplette IP-Subnetze eintragen.

> Wenn Sie diese Einstellung leer lassen, ist der Zugriff von überall aus erlaubt. Dies sollten Sie aus Sicherheitsgründen nicht tun, wenn Sie keine Firewall haben, die entsprechende Zugriffe aus dem Internet blockt.

Den Benutzernamen und das Passwort können Sie frei wählen. Aktivieren Sie aus Sicherheitsgründen wenn möglich immer SSL (POP3/S), da sonst Daten (insbesondere Benutzername und Passwort) protokollbedingt unverschlüsselt über Ihr Netzwerk versendet werden.

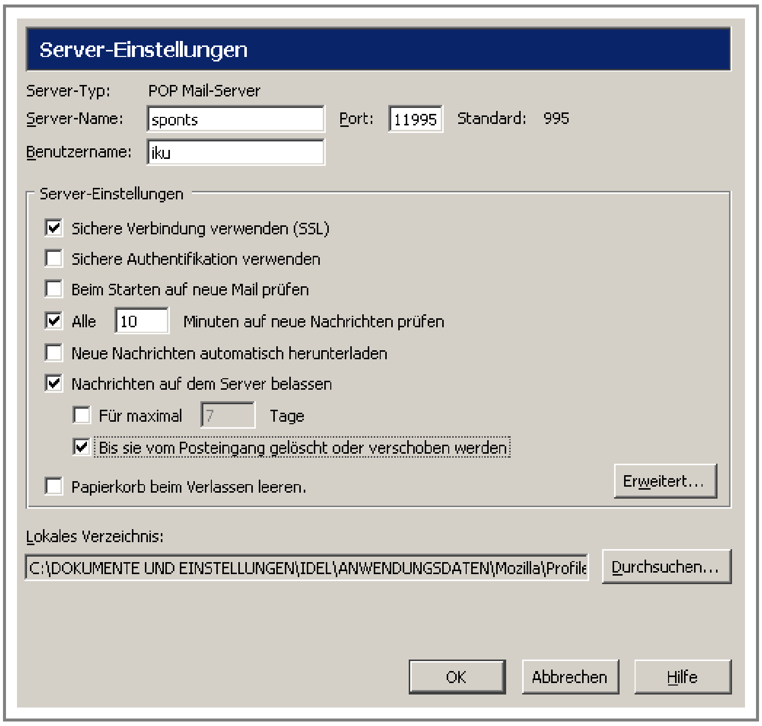


Abbildung 27: Einstellungen POP3-Abruf für Mozilla-Mail

Standardmäßig arbeitet POP3/S über den Port 995. Aus Sicherheitsgründen ist SPONTS im Auslieferungszustand auf Port 11995 eingestellt, damit Viren und Würmer ihn nicht finden und damit keine unnötige CPU-Last erzeugen. Ansonsten spricht nichts dagegen, wenn Sie diesen auf 995 stellen möchten.

7.7 Journal

Menüpunkt: *'Journal'*

Das Journal enthält einen Eintrag für jede eingegangene und auch jede abgewiesene Mail. Über den Navigationspunkt *'Journal'* erhalten Sie alle vorhandenen Einträge. Die Spalte *'Status'* enthält Informationen über den Zustand der Mail und kann einen der folgenden Werte annehmen:

- *'aborted' / abgebrochene E-Mails*
  Der Versender hat die Verbindung getrennt, bevor die Nachricht vollständig übermittelt wurde.
- *'blocked' / geblockte E-Mails*
  Die eingegangene E-Mail wurde blockiert. Gründe für das Blockieren der E-Mail können über die Details der E-Mail eingesehen werden und sind unter dem Punkt 'Reason' vermerkt.
- *'queued' / E-Mails in Warteschlange*
  Die Nachricht wurde in die Warteschlange eingestellt und wartet auf Zustellung zum entsprechenden Backend oder E-Mail Server.

- *'delivered' / zugestellte E-Mails*
  Die Nachricht wurde erfolgreich an das Backend oder den E-Mail Server ausgeliefert.
- *'exception' / Fehler bei der Verarbeitung*
  Bei der Verarbeitung ist in SPONTS ein nicht abgefangener Fehler auftreten. Gründe dieses Fehlers können über die Details der E-Mail eingesehen werden und sind unter dem Punkt 'Reason' vermerkt.

Sie haben hier – ähnlich wie beim Bearbeiten der Black/Whitelisten - die Möglichkeit, nach einzelnen Einträgen zu suchen. Dabei können Sie sich nach verschiedenen Kriterien suchen, müssen aber nicht alle angeben. Lassen Sie bei der Suche eines der Felder leer, so werden *alle* Ergebnisse für dieses Feld angezeigt.

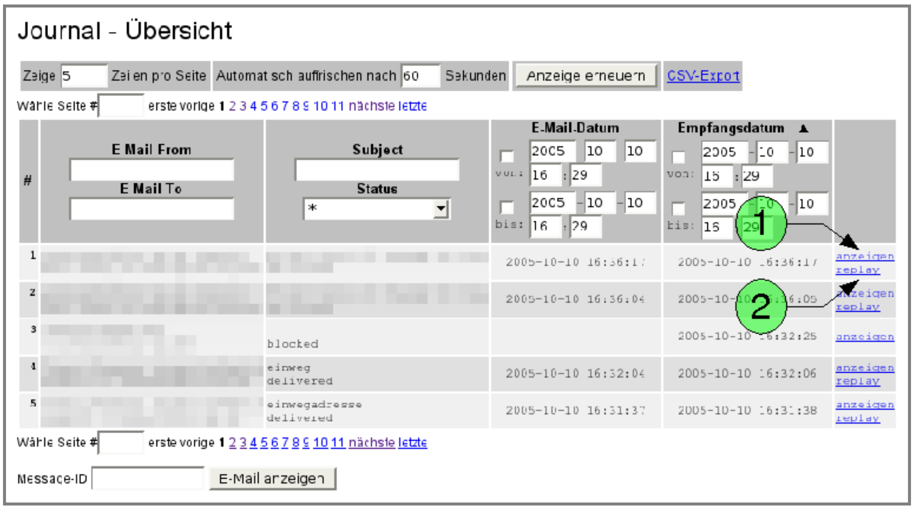


Abbildung 28: Journal-Übersicht

Klicken Sie bei der entsprechenden E-Mail auf den Link ① *'anzeigen'*, so erhalten Sie detaillierte Informationen zu dieser Mail. Bei Klick bei der entsprechenden E-Mail auf den Link ② *'replay'* wird die Mail über das Replay wieder als Mail in das System eingestellt.

7.7.1 Verbindungs- und Nachrichten-ID

Die eindeutige Verbindungs-ID besteht aus Hexadezimal-Zeichen, beispielsweise 'FAB9FC7A27'. Üblicherweise wird pro Verbindung nur jeweils eine Nachricht übertragen, aber insbesondere bei Mailinglisten können es auch mehrere sein. Jede Nachricht wird von 0 beginnend durchnummeriert, d.h. 'FAB9FC7A27-0' ist die erste Nachricht, die in der Verbindung 'FAB9FC7A27' übermittelt wurde. Diese IDs finden Sie auch in den Logdateien.

7.7.2 Einstellungen

Menüpunkt: '*Journal → Einstellungen*'

Hier können Sie Ober- und Untergrenze der Anzahl der Journaleinträge angeben. Sobald die Obergrenze erreicht ist, werden die ältesten Einträge aus dem Journal gelöscht, bis die Untergrenze erreicht ist.

- **Untere Schwelle der Zahl der Journal-Einträge**
  Wenn es mehr Protokoll-Einträge gibt als in der Oberen Schwelle festgelegt, löscht der Cron-Dienst so viele Einträge, bis weniger Einträge übrig sind als in dieser Einstellung festgelegt.
  Voreinstellung: `30000`
- **Obere Schwelle der Zahl der Journal-Einträge**
  Wenn es mehr Protokoll-Einträge gibt als in dieser Einstellung festgelegt, löscht der Cron-Dienst so viele Einträge, bis weniger Einträge übrig sind als in 'Untere Schwelle' festgelegt.
  Voreinstellung: `35000`

7.8 Replay

7.8.1 Replay verwenden

Menüpunkt: '*Replay*'

Das Replay bewahrt eine Kopie jeder eingegangenen Mail in einem Ringpuffer auf. Die Größe des Puffers wird durch die Festplattenkapazität bestimmt. Ist der Puffer voll, wird die jeweils älteste Kopie aus dem Puffer gelöscht, bis wieder genug Platz vorhanden ist.

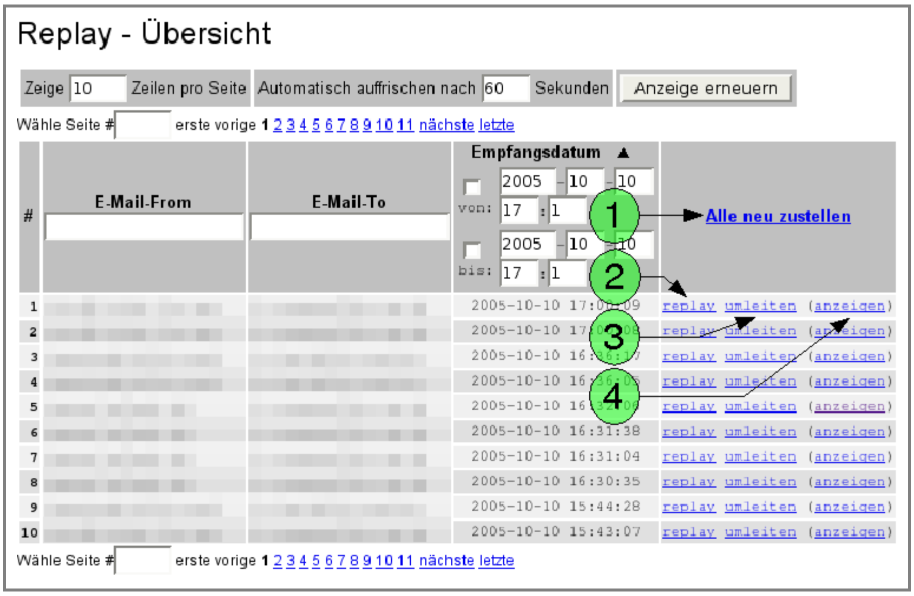


Abbildung 29: Auszug Replay

Geht eine einzelne Mail auf dem Backend oder beim Empfänger verloren - beispielsweise durch Viren oder Fehlbedienung - so kann sie über die Replay-Funktion beliebig oft erneut an das Backend versendet werden. Hierzu wählen Sie in der Web-GUI den Menüpunkt '*Replay*' an.

Sie haben hier – ähnlich wie beim Bearbeiten der Black/Whitelisten - die Möglichkeit, nach einzelnen Einträgen zu suchen. Dabei können Sich nach verschiedenen Kriterien suchen, müssen aber nicht alle angeben. Lassen Sie bei der Suche eines der Felder leer, so werden *alle* Ergebnisse für dieses Feld angezeigt.

In der Übersicht können Sie jetzt einzelne Mails durch einen Klick auf '*umleiten*' hinter der entsprechenden E-Mail erneut an das Backend schicken. Bei einem Klick

auf 'redirect' kann die Mail auch an ein anderes Postfach umgeleitet werden. Ist das Journal verfügbar, so kann durch einen Klick auf 'show' der entsprechende Eintrag im Journal eingesehen werden.

Gehen mehrere Mails verloren, so können diese ebenfalls erneut versendet werden. Hierzu schränken Sie zuerst die Ergebnismenge durch Eingabe von Absender (envfrom), Empfänger (envrcpt) und/oder Empfangsdatum (receiveddate) ein. Beim Empfangsdatum müssen Sie den Haken vor from (von) bzw. to (bis) setzen, damit die Einschränkung aktiv wird. Danach klicken Sie auf 'Refresh view' und prüfen, ob Sie die richtigen Nachrichten ausgewählt haben. Ist dies der Fall, so klicken Sie auf 'replay all' und alle ausgewählten Nachrichten werden - nach einer Sicherheitsabfrage - erneut versendet.

Achten Sie auf die Zahlenangabe oberhalb der Sicherheitsabfrage. Diese gibt an, wie viele Nachrichten bei 'replay all' versendet werden.

7.8.2 Einstellungen

Menüpunkt: '*Replay → Einstellungen*'

Hier können Sie Ober- und Untergrenze des freien Festplattenplatzes angeben. Sobald die Untergrenze erreicht ist, werden die ältesten Einträge aus dem Replay-Speicher gelöscht, bis die Obergrenze erreicht ist. Der freie Speicher sollte mindestens 10% der Festplattenkapazität betragen.

7.8.3 Replay-Admins

Menüpunkt: '*Replay → Replay-Admins*'

Die Liste der Replay-Administratoren kann an dieser Stelle geführt werden. Ein Replay-Administrator kann sich mit seinem Login und Kennwort an Ihrem SPONTS anmelden, erhält lediglich Zugriff auf das Modul Replay und kann E-Mails wieder in das E-Mailsystem einstellen.

Ein Replay-Administrator hat keinen Zugriff auf die Einstellungen des Replays oder auf die Liste der Replay-Administratoren.

7.9 Warteschlange

Menüpunkt: '*Warteschlange*'

Hier können Sie veranlassen, dass SPONTS versucht, alle Mails, die sich aktuell in der Warteschlange befinden, sofort auszuliefern. Dies ist oft sinnvoll, wenn das Backend nach einem Ausfall wieder zur Verfügung steht.

7.10 Systeminfo

Menüpunkt: '*Systeminfo*'

Hier erhalten Sie einige Informationen über den Systemstatus, die installierte Software und Lizenzen Ihres SPONTS.

7.10.1 Protokolle

Menüpunkt: '*Systeminfo → Protokolle*'

Über diesen Menüpunkt erhalten Sie eine Übersicht über die letzten protokollierten Meldungen Ihres SPONTS. Diese Meldungen sind in zeitlich absteigender

Reihenfolge sortiert, d.h. der aktuellste Eintrag befindet sich in der ersten Zeile.
Sie können alle protokollierte Meldungen über den Link *'Zip-Archiv'* in einer komprimierten Datei auf Ihrem Rechner speichern. Dies ist in Supportfällen wichtig, da in häufigen Fällen erst über die Konfiguration und protokollierte Meldungen Aussagen über den Grund eines Fehlverhaltens des SPONTS gemacht werden können.

7.10.2 Report

Die Reporte werden Ihnen nur dann angezeigt, wenn Sie eine gültige Lizenz für SPONTS-Report besitzen. Andernfalls werden Ihnen keine Liniendiagramme zu den erfassten Messdaten angezeigt, sie erhalten lediglich eine Anzeige des erreichten Maximalwertes über die y-Achse der Diagramme.

Die gesammelten Messdaten werden in täglicher, wöchentlicher, monatlicher und jährlicher Zusammenfassung als Liniendiagramme dargestellt.
Das Liniendiagramm der täglichen Übersicht zeigt die Daten der letzten 24 Stunden an, wobei ein Messpunkt einer Mittelung über 5 Minuten entspricht.
Das Liniendiagramm der wöchentlichen Übersicht zeigt die Daten der letzten Woche an, wobei ein Messpunkt einer Mittelung über 30 Minuten entspricht.
Das Liniendiagramm der monatlichen Übersicht zeigt die Daten des letzten Monats an, wobei ein Messpunkt einer Mittelung über 2 Stunden entspricht.
Das Liniendiagramm der jährlichen Übersicht zeit die Daten des letzten Jahres an, wobei ein Messpunkt einer Mittelung über 1 Tag entspricht.

E-Mail

Menüpunkt: *'Systeminfo ➔ E-Mail Report*'

Die Informationsseite E-Mail Report bietet über vier Grafiken einen Überblick über die Anzahl der von Ihrem SPONTS verarbeiteten E-Mail.
Als Messkurven werden die Anzahlen der als UCE erkannten, virenverseuchten, desinfizierten, normalen, sowie die Gesamtzahl der verarbeiteten E-Mails dargestellt.

UCE-Module

Menüpunkt: *'Systeminfo ➔ UCE-Module*'

Der Report der UCE-Module bietet einen Überblick über die Nutzung der einzelnen UCE-Module.

Verbindungen – Eingehend

Menüpunkt: *'Systeminfo → Verb.-Eing.*'

Der Report der eingehenden Verbindungen bietet einen Überblick über die Anzahl der eingehenden Verbindungen über SMTP, POP3 und IMAP.

Gleichzeitige ausgehende SMTP-Verbindungen

Menüpunkt: *'Systeminfo ➔ SMTP-Out*'

Der Report der gleichzeitig ausgehenden SMTP-Verbindungen bietet einen Überblick über die Anzahl gleichzeitiger SMTP-Verbindungen zum Backend und zu anderen E-Mail-Servern, an die SPONTS E-Mails weiterleitet.

Nutzung der Systemressourcen

Menüpunkt: *'Systeminfo → Ressourcen'*

Der Report der Nutzung der Systemressourcen bietet einen Überblick über die prozentuale Nutzung des Arbeitsspeichers des Systems.

Gleichzeitige Spamassassin Instanzen

Menüpunkt: *'Systeminfo → Spamassassin'*

Der Report der Nutzung gleichzeitiger Spamassassin-Instanzen bietet eine Übersicht über die Anzahl der gleichzeitig laufenden Instanzen des Spamassassin. Sollte diese Messkurve häufig den Maximalwert der gleichzeitigen Spamassassin-Instanzen erreichen, sollten Sie diese Einstellung (vgl. Max. Anzahl an Spamassassin-Instanzen, S.71) erhöhen, da Ihr SPONTS System zu lange auf freie Instanzen des Spamassassin wartet und der Durchsatz der verarbeiteten E-Mails beschränkt werden könnte.

7.10.3 Gleichzeitige Instanzen der Virenscanner

Menüpunkt: *'Systeminfo → Virusscanner'*

Der Report der gleichzeitigen Instanzen der Virenscanner bietet eine Übersicht über die Anzahl der gleichzeitig laufenden Instanzen der jeweiligen Virenscanner. Sollte diese Messkurve häufig den Maximalwert erreichen, sollten Sie entsprechende Einstellung (vgl. Max. Anzahl an Virenscannern, S. 52) erhöhen, da Ihr SPONTS zu lange auf freie Instanzen der Virenscanner wartet und der Durchsatz der verarbeiteten E-Mail beschränkt werden könnte.

8 Zugriff per SFTP

Zum Aufspielen von Updates und manuellen Ändern der Konfiguration verwenden Sie den SFTP-Zugriff.

Der Benutzername zum Zugriff per SFTP ist 'admin'; das Passwort entnehmen Sie der beiliegenden Kurzbeschreibung.

8.1 KDE

Unter KDE greifen Sie auf die URL sftp://admin@<ip-adresse>/ zu. Ist die IP-Adresse beispielsweise 192.168.0.100, so greifen Sie auf sftp://admin@192.168.0.100/ zu.

8.2 WinSCP

Unter http://winscp.sourceforge.net/ erhalten Sie die Software WinSCP.

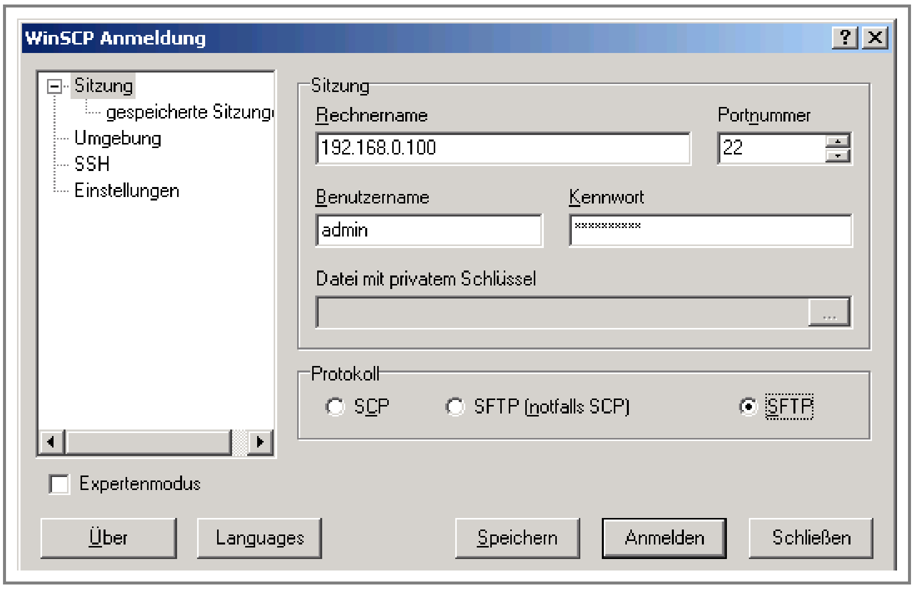


Abbildung 30: WinSCP

Geben Sie hier den Rechnernamen und als Benutzername 'admin' ein. Als Protokoll muss 'SFTP' eingestellt sein.

8.3 Verzeichnisstruktur

Nach dem Anmelden per SFTP erhalten Sie Zugriff auf die Festplatte von SPONTS. Wechseln Sie zuerst in das Unterverzeichnis '`/system`'. Hier sind alle Einstellungen und Dateien von SPONTS gespeichert.

8.3.1 /system/etc

Hier finden Sie Konfigurationsdateien des verwendeten Linux-Systems, sowie des SPONTS selbst. Sie können diese Dateien durch Kopieren auf Ihre lokale Festplatte sichern, sollten aber keine Veränderungen daran vornehmen.

8.3.2 /system/log

Hier werden Logdateien abgespeichert. SPONTS erzeugt standardmäßig 3 Logdateien mit einer Größe von jeweils maximal 4 MiB. Dies können Sie in der Datei
`/system/etc/sponts/Logging.properties`
anpassen.

8.3.3 /system/mods

Hier liegen die einzelnen Programmmodule von SPONTS.

> Alle in diesem Verzeichnis befindlichen Module werden verwendet, deshalb dürfen Sie die Module nur ersetzen! Wenn Sie Module umbenennen, löschen oder neue hinzufügen, kann es zu Fehlfunktionen kommen.

8.3.4 /system/spool

Hier finden Sie die Spooldateien der einzelnen Module, z.B. Warteschlange und Replay von SPONTS.

> Löschen Sie keine in diesem Verzeichnis vorhandenen Dateien, da es sonst zu Fehlfunktionen kommen kann.

8.3.5 /system/tmp

Dieses Verzeichnis enthält temporäre Dateien. Das Verzeichnis wird beim Booten von SPONTS automatisch gelöscht.

9 Zugriff per 'ssh'

Es besteht die Möglichkeit, als Benutzer 'root' per ssh auf die SPONTS Box zuzugreifen. Benutzen Sie hierzu einen SSH-Client. Unter Linux können Sie dazu das Kommando 'ssh' benutzen, für Windows müssen Sie einen geeigneten Client installieren, z.B. 'putty'.
Unter http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html erhalten Sie diese Software.

Wollen Sie von einem Linux Rechner aus auf den SPONTS zugreifen, geben Sie folgenden Befehl ein: ssh root@<IP Adresse des SPONTS>

Greifen Sie mithilfe der Software 'putty' auf den SPONTS zu, geben Sie die IP Adresse des SPONTS an und aktivieren Sie das Protokoll 'ssh'

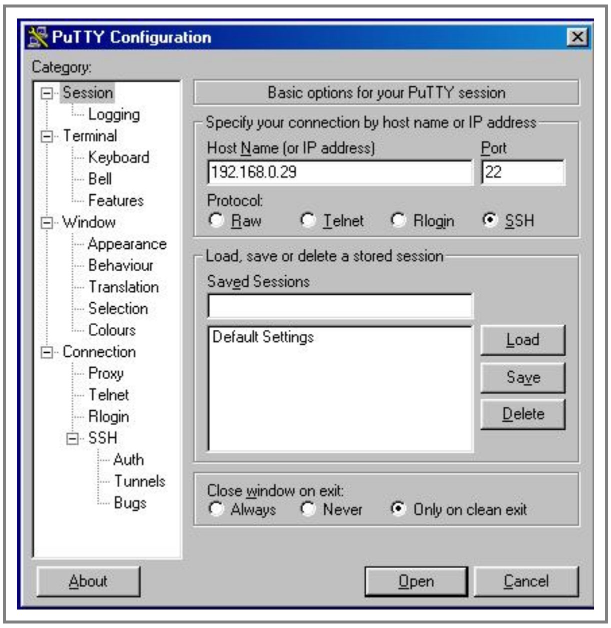


Abbildung 31: SSH-Verbindung mit 'putty'

Wenn Sie per ssh auf der SPONTS Box eingeloggt sind, haben Sie folgende Möglichkeiten:

- **SPONTS-Neustart (Neustart der SPONTS Software)**

```
killall java
```

- **SPONTS-Reboot (Neustart des kompletten Systems)**

```
init 6
```

- **SPONTS-Shutdown (Herunterfahren der SPONTS Box)**

```
init 0
```

Warnung: Nach der Eingabe des Shutdown-Befehls (`init 0`) schaltet sich die SPONTS-Box vollständig ab!

- **SPONTS-Neustart nach Update**

```
restart-sponts.sh
```

- **Werksseitige Einstellungen wieder herstellen**

```
reset_to_factory_defaults
```

> Achtung: Hiermit wird die komplette Datenbank und alle Einstellungen überschrieben. Alle Mails in Replay und in der Queue sowie der Lizenzschlüssel werden gelöscht!

- **Editieren der SPONTS-Einstellungen**
  Die Einstellungen des SPONTS sind in der Datei `Settings.properties` im Verzeichnis `/system/etc/sponts` gespeichert. Sie müssen diese Datei von Hand editieren, wenn Sie z.B. den Start der WEB-Gui deaktiviert haben und diese wieder aktivieren wollen.
  Zum editieren dieser Datei sollten Sie Grundkenntnisse im Umgang mit dem Texteditor *vi* besitzen.

9.1 Reaktivierung der WEB-Gui nach vorheriger Deaktivierung

1. Wechseln Sie zunächst in das Verzeichnis der SPONTS-Einstellungen:

```
cd /system/etc/sponts
```

2. Sichern Sie die Einstellungsdatei in einer Kopie, um diese noch im Originalzustand vorliegen zu haben, falls Probleme während des Editierens mit *vi* auftreten.

```
cp Settings.properties Settings.properties.orig
```

3. Starten Sie den Editor *vi*

```
vi Settings.properties
```

4. Suchen Sie die Zeile der Einstellung zum Start der WEB-Gui, indem Sie `/gui.web` *RETURN* eingeben.
5. Bewegen Sie den Cursor über die Pfeiltasten Ihrer Tastatur vor die Eintragung `no` am Ende der Zeile und löschen Sie dieses Wort über die Entfernen-Taste.
6. Wechseln Sie über die Taste `i` in den Eingabemodus des *vi* und geben Sie `yes` ein.
7. Speichern Sie die Datei und beenden Sie *vi*, indem Sie nacheinander die Tasten *ESC* `:` `x` *RETURN* drücken.
8. Starten Sie SPONTS nun neu

```
killall java
```

Falls Ihnen Fehler unterlaufen sind, oder Sie Änderungen an der Datei vorgenommen haben, die Sie nicht wünschen, können Sie *vi* ohne zu speichern über die Tastenfolge *ESC* `:` `q` `!` *RETURN* beenden

10 Updates

Zum Aufspielen von Updates benötigen Sie SFTP-Zugang (vgl. 8 Zugriff per SFTP, S.83). Speichern Sie die `.mod`-Dateien in dem Verzeichnis `/system/mods`, wobei Sie die jeweils bereits existierende Version ersetzen müssen.

> Alle in diesem Verzeichnis befindlichen Module werden verwendet, deshalb dürfen Sie die Module nur ersetzen! Wenn Sie Module umbenennen oder neue hinzufügen oder vorhandene Module löschen, kann es zu Fehlfunktionen kommen.

Nach dem Aufspielen müssen Sie einen Reboot auslösen. Dies können Sie über die Web-GUI oder auf der Kommandozeile durchführen.

11 Lizenzschlüssel installieren

Zum Aufspielen von Updates benötigen Sie SFTP-Zugang (vgl. Kap. 8 Zugriff per SFTP, S. 83).

11.1 SPONTS

Die Lizenzdatei muss in dem Verzeichnis `/system/etc/sponts` unter dem Namen `sponts-license.key` gespeichert werden. Danach muss SPONTS neu gestartet werden.

11.2 H+BEDV Antivir

Die Lizenzdatei muss in dem Verzeichnis `/system/spool/antivir` unter dem Namen `hbedv.key` gespeichert werden. Danach muss SPONTS neu gebootet werden.

11.3 Sophos

Für den Virenschutz von Sophos wird Ihnen ein Zugang mit Benutzernamen und Passwort zur Verfügung gestellt. Diese Zugangsdaten müssen Sie in die Datei `/system/etc/sophos/sophos-update.cfg` eintragen. Die entsprechenden Felder stehen direkt am Anfang der Datei. Die anderen Parameter in dieser Konfigurationsdatei sollten Sie nicht ändern! Falls Sie einen HTTP-Proxy verwenden müssen Sie diesen (und evtl. auch Benutzernamen und Passwort dafür) ebenfalls angeben. Die Datei könnte beispielsweise wie folgt aussehen:

```
# Web login data (download, not EM download!)
export SavWebLogin=spohosloginname
export SavWebPasswd=geheim

# Proxy details in the format 'http://<ip>:<port>'; leave empty for
no proxy
export http_proxy=http://proxy:3128
# Username/password for proxy-authentication; leave empty for no
authentication
export ProxyUser=proxyloginname
export ProxyPassword=geheimproxy
# Filename for LINUX to download without any extension
export Lname=linux.intel.libc6.glibc.2.2
# first extension for LINUX (default tar)
export Lext1=tar
# Second extension for LINUX
export Lext2=Z
```

Weitere Konfigurationen zum Sophos Virenscanner können Sie außerdem in den Dateien
`/system/etc/sophos/sophie.savi`
und
`/system/etc/sophos/sophie.cfg`
vornehmen. Beachten Sie aber, dass Änderungen in diesen Dateien die Funktionsweise des kompletten SPONTS beeinträchtigen können.

12 SPONTS Intern

12.1 Direktzugriff auf die SQL-Datenbank

Datenbank-Typ:	MySQL 3.x
Port:	3306
Datenbank:	sponts
Benutzername:	admin

SPONTS verwendet eine MySQL-Datenbank zur Speicherung der Empfänger, Black-/Whitelisten, des Journals und vielem mehr. Durch den direkten Zugriff auf die Datenbank können Sie - entsprechende SQL-Kenntnisse vorausgesetzt - leicht eigene Auswertungen nach Ihren Bedürfnissen erstellen. Auch können Sie SPONTS in Ihre eigenen Infrastruktur integrieren, indem Sie statt mit der Web-GUI zu arbeiten, direkt die entsprechenden Tabellen ändern.

12.1.1 JDBC (z.B. Java, OpenOffice)

Eine genaue Erklärung der Installation finden Sie unter:
http://www.mysql.de/doc/de/Java.html

12.1.2 ODBC (z.B. Microsoft Access)

Eine genaue Erklärung der Installation finden Sie unter:
http://www.mysql.de/doc/de/ODBC.html

12.1.3 Kurzeinführung in SQL

SQL ist eine deklarative Datenbanksprache für Relationale Datenbanken und besitzt eine relativ einfache Syntax, die an die englische Umgangssprache angelehnt ist.
Durch SQL wird eine Reihe von Befehlen zur Definition von Datenstrukturen, zur Manipulation von Datenbeständen (Anfügen, Bearbeiten und Löschen von Datensätzen) und zur Abfrage von Daten und zur Verwaltung der Zugangskontrolle zur Verfügung gestellt.
Im Folgenden wird eine kurze Beschreibung Befehlen der Datenbankabfrage und Datenmanipulation gegeben, eine genauere Erklärung der Datenbanksprache SQL finden Sie z.B. unter:
http://de.wikipedia.org/wiki/Sql

Datenbankanfragen: SELECT

Die SELECT-Anweisung startet eine Abfrage. Aufgrund der Syntax kann eine SELECT-Anweisung auch als "SFW-Block" (SELECT, FROM, WHERE) bezeichnet werden. Syntax (unvollständig):

```
SELECT Auswahlliste
FROM Quelle
WHERE Where-Klausel
[ORDER BY (Sortierungsattribut)+ [ASC|DESC]]
```

- *Auswahlliste* bestimmt, welche Spalten der *Quelle* auszugeben sind (* für alle) und ob Aggregatfunktionen anzuwenden sind.
- *Quelle* gibt an, wo die Daten herkommen. Es können Relationen und Sichten angegeben werden und miteinander als kartesisches Produkt oder

als Verbund (JOIN, ab SQL-92) verknüpft werden. Mit der zusätzlichen Angabe eines Namens können Tupelvariablen besetzt werden, d.h. Relationen für die Abfrage umbenannt werden (vgl. Beispiele).

- *Where-Klausel* bestimmt Bedingungen, unter denen die Daten ausgegeben werden sollen. In SQL (außer MySQL <=3) ist hier auch die Angabe von Unterabfragen möglich, so dass SQL *streng relational vollständig* wird.
- *Sortierungsattribut*: nach ORDER BY werden Attribute angegeben, nach denen sortiert werden soll. ASC gibt dabei aufsteigende (Standard), DESC absteigende Sortierung an. Ein Sortierungsattribut muss **nicht** in der Auswahlliste vorkommen.

Beispiele

```
SELECT * FROM validrecipients;
```

- Listet alle Werte aller Spalten aus der Tabelle validrecipients auf.

```
SELECT ip FROM attachmentfilter;
```

- Projektion: Listet nur die Spalte ip aus der Tabelle attachmentfilter.

```
SELECT sender,recipient FROM attachmentfilter WHERE hits > 100;
```

- Selektion: Listet die Spalten sender und recipient aus der Tabelle attachmentfilter auf, die mehr als 100-mal genutzt wurden.

```
SELECT COUNT(*) FROM journal WHERE status='blocked' recipient LIKE
'%jboke.de' AND maildate<20062001 AND maildate>20061001;
```

- Aggregation: Anzahl aller Einträge der Tabelle journal, deren Status 'blocked' , Empfänger 'jboke.de' ist und die zwischen dem 10.01.2006 und 20.01.2006 empfangen wurden.

Datenmanipulation: INSERT und DELETE

Zur Datenmanipulation stehen die Befehle INSERT und DELETE zur Verfügung:

```
INSERT INTO Relation ['(' (Attribut)+ ')'] VALUES
'('(Konstanten)+')'
INSERT INTO Relation ['(' (Attribut)+ ')'] SFW-Block
DELETE FROM Relation [WHERE Where-Klausel]
```

- Mit INSERT können explizit konstruierte Tupel oder die Ergebnisse eines SFW-Blocks in eine Relation eingefügt werden.
- Wird bei DELETE die WHERE-Klausel weg gelassen, wird die *ganze* Relation gelöscht, aber nicht das Schema.

Beispiele

```
INSERT INTO validrecipients (recipient) VALUES ('@jboke.de');
```

- Fügt eine Zeile mit dem gegebenen Empfänger in die Tabelle validrecipients ein.

```
DELETE FROM autoblacklist WHERE sender LIKE '%jboke.de';
```

- Entfernt alle Einträge aus der Tabelle autoblacklist, deren Einträge im Feld sender auf 'jboke.de' enden.

Datendefinition: CREATE, ALTER, DROP

Zugangkontrolle: GRANT und REVOKE

12.1.4 Beschreibung SQL-Tabellen

Fett geschriebene Felder sind Primärschlüssel

attachmentfilter: Filterung von E-Mail Angängen

(vgl. 7.3.7 Anhang, S. 59 ff.)

ip	**varchar(45)**	**IP-Nummer des sendenen SMTP-Servers**
sender	**varchar(200)**	**E-Mail Adresse oder Domain des Senders**
recipient	**varchar(200)**	**E-Mail Adresse oder Domain des Empfängers**
policy	enum('accept','reject')	Vorgehensweise
extensions	varchar(255)	Liste der Dateinamenerweiterungen, mit Komma getrennt
listdate	datetime	Zeitpunkt des Listeneintrags
lasthit	timestamp(14)	Zeitpunkt des letzten Treffers auf diesem Eintrag
hits	int(11)	Anzahl der bisherigen Treffer auf diesem Filter

autoblacklist: Automatische Schwarze Liste

(vgl. 7.5.2 Auto-Blacklist, S. 73 ff.)

ip	**varchar(45)**	**IP-Nummer des sendenen SMTP-Servers**
sender	**varchar(200)**	**E-Mail Adresse oder Domain des Senders**
listdate	datetime	Zeitpunkt des Listeneintrags
lasthit	timestamp(14)	Zeitpunkt des letzten Treffers auf diesem Eintrag
hits	int(11)	Anzahl der bisherigen Treffer

cache

(vgl. 7.4.3 Cache löschen, S. 62)

type	**int(11)**	**0: IMMUNEHOST** **1: gültige Domain** **2: gültiger Absender** **3: gültiger SPF Sender** **4: authentisierter Benutzer** **5: Empfänger mit temporärem Whitelisting**
id	**varchar(255)**	
value	varchar(255)	
listdate	datetime	Zeitpunkt des Eintrags

disinfectionoptin: Einwilligung zur E-Mail-Desinfektion

(vgl. 7.3.12 Virenscanner / E-Mail Desinfektion, S. 61)

recipient	**varchar(200)**	**Empfängeradresse oder Domain der Einwilligung**

disposableoptin: Einwilligung zur Nutzung von Einwegadressen

(vgl. 7.5.4 Einwilligung zu Einwegadressen, S. 75)

recipient	**varchar(200)**	**Empfängeradresse oder Domain der Einwilligung**

disposablerecipients: Einwegadressen und Empfänger

(vgl. 7.5.4 Einwegadresse und Empfänger, S. 74)

keyword	**varchar(200)**	**Schlüsselwort der Einwegadresse**
recipient	**varchar(200)**	**Empfängeradresse**
maxvalue	int(11)	Maximalzahl der empfangbaren E-Mails
remaining	int(11)	verbliebene Anzahl empfangbarer E-Mails
forwarded	int(11)	Gesamtzahl der weitergeleiteten E-Mails
blocked	int(11)	Anzahl der geblockten E-Mails
listdate	datetime	Zeitpunkt des ersten Auftretens der Einwegadresse
lasthit	datetime	Zeitpunkt des letzten Treffers der Einwegadresse

domainadmin: Domainspezifische Administratoren

(vgl. 7.3.8 Domain-Admins, S. 60)

domain	**varchar(200)**	**Domain, welche über diesen Zugang administriert wird**
password	varchar(40)	SHA1-Hash des Passworts
mailaddress	varchar(200)	E-Mail Adresse des Domain-Administrators

In der Tabelle domainadmin muss der SHA1-Hashwert des Domainadmin-Passwortes gespeichert werden.

envelopepolicy: Black- und Whitelisting

(vgl. 7.3.6 Envelope, S. 58ff.)

ip	**varchar(45)**	**IP-Nummer des sendenen SMTP-Servers**
sender	**varchar(200)**	**E-Mail Adresse oder Domain des Senders**
recipient	**varchar(200)**	**E-Mail Adresse oder Domain des Empfängers**
policy	enum('accept', 'reject', 'never-reject', 'noscan', 'spamtrap', 'allow-encrypted')	Vorgehensweisen 'accept' : annehmen 'reject' : zurückweisen 'never-reject' : niemals zurückweisen 'noscan' : nicht auf Viren prüfen 'spamtrap' : Postfach ist eine Spamfalle 'allow-encrypted' : verschlüsselte Dateien erlauben
listdate	datetime	Zeitpunkt des Eintrags
lasthit	timestamp(14)	Zeitpunkt des letzten Treffers
hits	int(11)	Anzahl der Treffer auf dem Eintrag

ftpuser: Logins des FTP-Proxy (optional)

user	**varchar(20)**	**Benutzername**
password	**varchar(20)**	**Passwort**

journal

(vgl. 7.7 Journal, S. 77)

id	**varchar(20)**	**Eindeutige ID des Journal-Eintrages**
ip	varchar(45)	IP-Nummer des sendenen SMTP-Servers
sender	text	E-Mail Adresse des Senders (SMTP 'MAIL FROM:')
recipient	text	E-Mail Adresse des Empfängers (SMTP 'RCPT TO:')
mailsender	text	E-Mail Adresse des Senders (aus E-Mail Header 'sender:')
mailfrom	text	E-Mail Adresse des Senders (aus E-Mail Header 'from:')
mailto	text	E-Mail Adresse des Empfängers (aus E-Mail Header 'to:')
cc	text	E-Mail Adresse(n) weiterer Empfängers (aus E-Mail Header 'cc:')
bcc	text	E-Mail Adresse(n) für Blindkopien
replyto	text	Antwort E-Mail Adresse (aus E-Mail Header 'replyto:')
maildate	datetime	Datum und Uhrzeit der E-Mail (aus E-Mail Header 'date:')
receiveddate	datetime	Datum und Uhrzeit der E-Mail (Ankunftszeitpunkt bei SPONTS)
subject	text	Betreff der E-Mail (aus E-Mail Header 'subject:')
totallength	bigint(20)	Gesamtlänge der E-Mail in Bytes
attachments	text	Name der Attachments
spamscore	double	Gesamtspamscore der E-Mail
status	enum('aborted', 'blocked', 'queued', 'delivered', 'undelivered', 'deleted', 'exception')	'aborted': Versenden der Mail wurde abgebrochen 'blocked': Mail wurde vom System blockiert 'queued': Weiterleitung der Mail fehlgeschlagen, wird noch in der Warteschlange gehalten 'delivered': Mail zugestellt 'undelivered': Mail nicht zugestellt 'deleted': vom Administrator aus der Warteschlange gelöscht 'exception' : Ausnahmezustand während der E-Mail Verarbeitung
reason	text	Grund für Status

Die Einträge in diese Tabelle werden vom System generiert. Es dürfen keine Journaleinträge manuell hinzufügt oder verändert werden!

localdomains

(vgl. 7.3.2 Lokale Domains, S. 57)

domain	**varchar(200)**	**Domains, für die E-Mail empfangen wird**

monitorproxies

(vgl. 7.3.9 Proxies, S. 61)

ip	**varchar(45)**	**IP-Nummer, auf der auf eingehende Verbindungen gewartet werden soll**
port	**int (11)**	**Port-Nummer, auf der auf eingehende Verbindungen gewartet werden soll**
usessl	enum('yes', 'no')	SSL bei der eingehenden Verbindungen nutzen
upstreamip	varchar	IP-Nummer des Backends
upstreamport	int	Port-Nummer des Backends
upstreamssl	enum('yes', 'no')	Verbindung zum Backend mit SSL-Verschlüsselung
type	enum('smtp', 'imap', 'pop3')	Typ der Verbindung
id	varchar(40)	
sslcertificatepath	varchar(200)	Pfad zum SSL-Zertifikat des Backends

rcptrewrite: Empfänger-Ersetzungsregeln

(vgl. 7.3.4 Empfänger ersetzen, S. 57)

recipient	**varchar(200)**	**E-Mail Adresse oder Domain des Empfängers**
newrecipient	varchar(200)	neuer Empfänger oder Domain
mode	enum('redirect', 'copy')	redirect : Umschreiben des Empfängers auf neuen Empfänger copy : Kopie an neuen Empfänger

recipientbackend: Empfängerspezifische Backends

(vgl. 7.3.5 Backend je Empfänger, S. 57)

recipient	**varchar(200)**	**E-Mail Adresse oder Domain des Empfängers**
backendhost	varchar(200)	IP-Adresse oder DNS-Name des SMTP-Backends
backendport	int(5)	Portnummer des SMTP-Backends
usessl	enum('yes', 'no')	SSL gesicherte Verbindung
login	varchar(200)	Login am Backend zur Authentifizierung am Backend
password	varchar(200)	
method	enum('PLAIN', 'LOGIN', 'CRAM-MD5', 'CRAM-SHA1')	Authentisierungsmethode

Für die Authentifizierungsmethoden CRAM-MD5 und CRAM-SHA1 muss ein Passwort angegeben werden. Andernfalls kann über diese Methode nicht authentifiziert werden.

recipientkeys: Zufällige temporäre Schlüssel zur Benutzeranmeldung

recipient	**varchar(200)**	**E-Mail Adresse oder Domain des Empfängers**
password	varchar(24)	zufälliger temporärer Schlüssel für Benutzeranmeldung
created	datetime	Zeitpunkt der Erzeugung

Die Einträge in dieser Tabelle werden vom System generiert und verwaltet.

recipientstatistic: Domain- und Empfängerspezifische Mailstatistiken

recipient	**varchar(200)**	**E-Mail Adresse oder Domain des Empfängers**
reportday	**date**	**Zeitpunkt des Reporteintrags**
delivered	int(11)	Anzahl der zugestellten Mails
queued	int(11)	Anzahl der in die Warteschlange eingestellten Mails
aborted	int(11)	Anzahl der nicht zustellbaren Mails
blocked	int(11)	Anzahl der geblockten Mails
virused	int(11)	Anzahl der von Virenscannern gemeldeten Mails
undelivered	int(11)	Anzahl der unzustellbaren Mails
disinfected	int(11)	Anzahl der desinfizierten Mails

Die Einträge in dieser Tabelle werden vom System generiert und verwaltet.

replayadmin: Liste der Replay-Administratoren

(vgl. 7.8.3 Replay-Admins, S. 80)

login	**varchar(200)**	**Login des Replay-Administrators**
password	varchar(200)	Passwort

replaylog: Daten der Mails im Replay-Ringpuffer

path	**varchar(100)**	**Pfad im Dateisystem**
sender	text	E-Mail Adresse oder Domain des Senders
recipient	text	E-Mail Adresse oder Domain des Empfängers
receiveddate	datetime	Datum und Uhrzeit der E-Mail (Ankunftszeitpunkt bei SPONTS)
Die Einträge in dieser Tabelle werden vom System generiert und verwaltet.		

statisticoptin: Empfänger der Mailstatistiken

(vgl. 7.3.11 Statistik, S. 61)

recipient	**varchar(200)**	**E-Mail Adresse oder Domain des Empfängers**

uceoptin: UCE-Einwilligung für E-Mail Adressen und Domains

(vgl. 7.5.3 UCE Opt-In / UCE-Einwilligung, S. 73)

recipient	**varchar(200)**	**E-Mail Adresse oder Domain des Empfängers**

users: Logins zur SMTP-Authentifizierung am SPONTS

(vgl. 7.3.10 Benutzer, S. 61)

login	**varchar(200)**	**Login**
password	varchar(200)	Passwort

validrecipients: Gültige Empfängeradressen und Domains

(vgl. 7.3.1 Empfänger,S. 56)

recipient	**varchar(200)**	**E-Mail Adresse oder Domain des Empfängers**

12.2 Mail-Warteschlange

(vgl. 7.9 Warteschlange, S. 80)

Die Warteschlange liegt im Verzeichnis

`/system/spool/sponts`

Jede Mail wird auf bis zu 4 Dateien aufgeteilt, die als Dateinamen die ID der E-Mail plus eine der folgenden Endungen haben:

.0: Envelope- und Verwaltungsinformationen

.1: Mail-Text

.2: vom SPONTS hinzugefügte Headerzeilen

.3: Empfänger, bei denen die Zustellen temporär nicht geklappt hat (optional)

Dieses Verzeichnis wird alle 'Wartezeit zwischen Sendeversuchen (Sek.)' (S. 50) Sekunden durchgesehen und alle darin enthaltenen Mails, die älter als 'Mindestalter in der Warteschlange (Sek.)' (S. 50) sind, an die SPONTS-Programm-interne Sende-Queue angehangen. Neue Mails werden direkt an diese Queue angehangen.

☞ Man kann Verzeichnisse erzeugen und Mails in diese. Die verschobenen E-Mails werden dann nicht mehr zugestellt, erscheinen aber im Journal noch als 'queued', da das Verschieben keinen Einfluss auf die SQL-Datenbank hat.

Beispielproblem: Backend hat eine Größenbeschränkung, SPONTS nicht.
Folge: Mails bleiben auf dem SPONTS liegen und verstopfen die Warteschlange, da neue Mails hineinkommen, aber jedesmal versucht wird, die zu großen Mails zuzustellen.

Lösung:

a) 'Maximale E-Mail Größe (in Bytes) (S. 47)' am SPONTS einstellen (greift sofort) oder diese am Backend entfernen

b) anderes Backend einstellen (greift sofort)

13 Problembehebung und FAQ

13.1 Zu wenig Spam gefiltert

Fehler: Eine Mail wurde nicht gefiltert, obwohl sie eine eindeutige Spam-Mail ist.

Lösung: Im Journal die entsprechende Mail aufrufen (show) und dort prüfen, welche Punktzahl erreicht wurde. Ist diese auf 0.0, so kann es sein, dass eine Whitelist aktiv wurde. Beispielsweise eine Whitelist für einen Backup-MX. Prüfen Sie hierzu die Absende-IP-Adresse.

Achten Sie auch darauf, ob Zensoren aktiviert sind, als Bewertungsfaktor bei diesen allerdings 0 eingetragen ist. Sollten diese Zensoren eine positive Erkennung einer UCE durchführen, wird ihr Ergebnis in die Gesamtsumme der Zensoren ebenfalls mit 0 einfließen und so keine Wirkung zeigen.

13.2 Backend ausgefallen

Fehler: Das Backend ist ausgefallen uns SPONTS soll alle in der Zwischenzeit eingehende E-Mails puffern.

Lösung: Damit die gepufferten E-Mails wegen des Backend-Ausfalls nicht frühzeitig als unzustellbar geblockt werden, müssen Sie kurzzeitig die Maximale gesamte E-Mail Zustellungsdauer (Sek.) (S. 50) erhöhen. Diese Einstellung ist im Auslieferungszustand auf 432000 Sekunden (5 Tage) eingestellt. E-Mails, welche länger als diese Zeitdauer in der Warteschlange verweilen, werden als unzustellbare E-Mails behandelt. Tragen Sie an dieser Stelle eine höhere Maximalzeit, z.B. 864000 Sekunden (10 Tage) ein. Achten Sie darauf, dass diese Zeiten in Sekunden angegeben werden müssen und nicht unter der Ausfallzeit Ihres Backends liegt.
Während der Ausfallzeit Ihres Backends sollten Sie zudem die Zwischenspeicher des SPONTS von Zeit zu Zeit überprüfen. Sobald die Spoolverzeichnisse keinen Speicherplatz mehr bieten, kann Ihr SPONTS keine E-Mails mehr puffern. Falls der Speicherplatz in diesen Verzeichnissen knapp wird, können Sie angesammelte Dateien aus den Spoolverzeichnissen über SFTP-Zugriff auf einen anderen Rechner verschieben und nach Wiederinbetriebnahme des Backends in diese Verzeichnisse zurück kopieren.

Nachdem Sie Ihr Backend wieder in Betrieb genommen haben, sollten Sie SPONTS dazu veranlassen, die in der Warteschlange angesammelten E-Mails zu versenden (vgl. 7.9 Warteschlange, S. 80). Klicken Sie dazu im Menü auf den Eintrag '*Warteschlange*' und in der erscheinenden Seite auf den Knopf '*Warteschlange abarbeiten*'.
Nachdem die gesammelten E-Mails aus der Warteschlange abgearbeitet wurden, sollten Sie die zuvor geänderte Einstellung Maximale gesamte E-Mail Zustellungsdauer (Sek.) wieder auf ihren Anfangswert setzen.

Falls Sie das Modul UMS haben, können Sie zudem jederzeit währen der Ausfallzeit Ihres Backends über den UMS-Zugang auf die eingegangenen E-Mails zugreifen und diese Ihren Nutzern zukommen lassen (vgl. 7.6 UMS, S. 75ff).

13.3 Wie überprüft man, ob SPONTS noch „lebt"?

Zur Überprüfung, ob SPONTS noch arbeitet, können Sie dies auf seinem SMTP-Port einen Verbindungsversuch z.B in einem Shellskript testen.

13.4 E-Mails des Backup-MX werden geblockt

Fehler: Eingehende E-Mails, welche von einem Backup-MX kommend eingehen werden geblockt.

Lösung: Oftmals halten E-Mails, welche über einen Backup-MX versendet werden einer SPF-Überprüfung (vgl. Sender Policy Framework, S. 67) nicht stand und werden abgelehnt, da häufig der Backup-MX nicht im SPF-Eintrag der entsprechenden Domain zugelassen wird.
Um E-Mails, welche von diesen Servern kommen annehmen zu können, tragen Sie die IP-Adresse des Backup-MX in der Tabelle Envelope (S. 58) mit der Regel 'niemals zurückweisen / never reject' ein.

Allgemein sollte der SPF-Eintrag der Domain des Backup-MX diesen mit als zulässige E-Mail Server angeben.

14 SPONTS/Monitor (TKÜV)

SPONTS/Monitor erlaubt die Überwachung von E-Mail-Kommunikation nach den Richtlinien der Telekommunikationsüberwachungsverordnung (TKÜV). Hierzu werden die Protokolle

- SMTP, SMTP/S, SMTP mit TLS
- IMAP, IMAP/S, IMAP mit TLS
- POP3, POP3/S, POP3 mit TLS

überwacht und gegebenenfalls die geforderten Datensätze erzeugt und an die berechtigte Stelle übermittelt.

Diese Anleitung ist kein Ersatz für das Lesen der TKÜV und der entsprechenden Technischen Richtlinie! iKu hat die hier beschriebenen Maßnahmen und Vorgehensweisen sorgfältig geprüft, bietet jedoch keinerlei Gewähr für deren Richtigkeit.

14.1 Funktionsweise

Die Überwachung von SMTP erfolgt in einem eigenen Milter, der über jede durchgeleitete E-Mail informiert wird. Deshalb ist hierfür keine eigene Konfiguration notwendig. Die Überwachung von IMAP/POP3 erfolgt über entsprechende Proxies, die unabhängig vom SMTP-Server arbeiten.

14.2 Einbindung

Der komplette E-Mail-Verkehr muss über SPONTS geleitet werden. Dies umfasst sowohl den Empfang und Versand von Mails per SMTP, als auch den Abruf per POP3 oder IMAP sowie das Hochladen von Mails in IMAP-Ordner. Hierbei muss auch die IP-Adresse der Gegenstelle protokolliert werden.

14.2.1 Einbindung von SMTP

SMTP-Server werden über die Standard-SMTP-Engine vom SPONTS angebunden. Diese unterstützt den Empfang und den Versand von E-Mails.

14.2.2 Einbindung von IMAP/POP3

IMAP- und POP3-Server werden über den IMAP- bzw. POP3-Proxy eingebunden. Dieser reicht Befehle des Clients transparent an den eigentlichen Server (hier „Upstream“ genannt) weiter und ebenso die Antworten des Servers an den Client. E-Mail-Abrufe werden automatisch erkannt und mit den aktuellen Überwachungsmaßnahmen abgeglichen und ggf. die entsprechenden Daten an die berechtigte Stelle ausgeleitet.

In der Konfigurationsdatei können Sie jeweils einen Upstream-Server für IMAP und POP3 angeben. Haben Sie mehr Server, so können Sie diese in der Tabelle 'Proxies' definieren. Hierbei müssen Sie auf dem SPONTS jeweils eine eigene IP-Adresse und/oder Port angeben. In der Spalte 'SSL' definieren Sie, ob SSL verwendet werden soll.

Da die Konfiguration von SPONTS nur eine IP-Adresse kennt, müssen Sie weitere IP-Adressen sowie die entsprechenden Routing-Einträge in der Datei

/system/etc/boot.local

über die Linux-Befehle 'ifconfig' und 'route' selbst definieren.

14.3 Einsatzszenarien und Beispiele

14.3.1 Allgemeine Voraussetzungen

Alle Szenarien haben gemeinsam, dass SPONTS für alle Verbindungen als Proxy zwischen dem Client (bzw. sendenden Mail-Server) und dem eigentlichen Mailserver (Backend) geschaltet wird. Wichtig ist hierbei, dass der Client bzw. sendende Mailserver keine Möglichkeit erhält, an SPONTS vorbei auf den ursprünglichen Mailserver zuzugreifen. Dies bedingt auch, dass die Authentisierung von SPONTS durchgeführt wird. Hierfür müssen in SPONTS Parameter wie eigene Domains und 'trusted networks' angegeben werden.

Eine Ausnahme bildet hier lediglich die Sandwich-Technik, die weiter unten beschrieben wird. Hier wird ein Teil des ursprünglichen Mailservers, der dann auch die Authentisierung übernimmt, vor SPONTS geschaltet.

SSL und Zertifikate

SPONTS unterstützt beliebig viele SSL-Zertifikate. Um SSL zu verwenden, muss das Zertifikat im Tomcat keystore-Format vorliegen. Das Erzeugen eines Zertifikates ist in 4.4 Zertifikate (S. 12 ff) beschrieben.

Importieren eines bereits bestehenden Zertifikates

Wenn Sie bereits ein Zertifikat besitzen, das Sie benutzen wollen, müssen Sie es zunächst per SCP oder SFTP auf SPONTS (z.B. nach Verzeichnis /tmp/mycert.crt) kopieren. Dann können Sie das vorhandene Zertifikat konvertieren:

```
/system/mount/java/bin/keytool \
      -keystore /tmp/keystore.tmp -import -alias sponts \
      -file /tmp/mycert.crt
```

Installieren des SSL-Zertifikates

Als Ausgabedatei wurde zunächst '/tmp/keystore.tmp' gewählt, um bei einem Fehler nicht das schon bestehende Zertifikat zu überschreiben. Falls Ihnen bei der Zertifikatserstellung ein Fehler unterlaufen ist, müssen Sie die (fehlerhafte) Datei löschen, bevor Sie ein neues Zertifikat erstellen. (z.B. mit rm /tmp/keystore.tmp).

Hat die Erzeugung oder Konvertierung funktioniert, können Sie das bestehende Zertifikat ersetzen:

sh-2.05a# cp /tmp/keystore.tmp /system/etc/sponts/sponts.keystore

Falls Sie die Zertifikate auf einem anderen Rechner erzeugen oder konvertieren, müssen Sie noch den Pfad zum Programm 'keytool' im oben angebenden Beispiel ändern und anschließend die erzeugte keystore-Datei per SCP oder SFTP auf SPONTS nach /system/etc/sponts/sponts.keystore kopieren.

Verwenden mehrerer Zertifikate

1. Standardmäßig verwendet SPONTS immer das Zertifikat in dem oben angegebenen Keystore. Um weitere Zertifikate zu verwenden, müssen Sie diese auf den SPONTS kopieren und die entsprechenden Serverdienste in der

SPONTS-Konfiguration unter „Proxies“ anlegen. Legen Sie die Zertifikate auf dem SPONTS im Unterverzeichnis „/system/local“ ab, da alle anderen Verzeichnisse durch ein Update überschrieben werden können. Geben Sie dann in der Proxy-Konfiguration den vollständigen Pfad zu der Datei an.

14.3.2 SMTP

Umstellung Netzwerkinfrastruktur für eingehende Verbindungen

Umstellen MX oder DNS

In diesem Szenario wird der Eingang der E-Mails auf SPONTS umgestellt. Dies kann mit verschiedenen Methoden geschehen, welche aber für neue Konstellationen keinen Unterschied machen. Ziel ist es hier, dass der sendende Host aus dem Internet sich beim SMTP-Versand direkt mit SPONTS verbindet. SPONTS muss aber für jede dieser Möglichkeiten aus dem Internet auf Port 25 erreichbar sein. Die Umstellung eingehender Mail kann mit folgenden Methoden erreicht werden:

Beim Einsatz von mehreren SPONTS können auch mehrere MX-Einträge verwendet werden. Alle MX müssen auf einen SPONTS/Monitor zeigen. Beachten Sie, dass eine DNS-Umstellung immer einige Zeit braucht, bis sie jedem sendenden Host bekannt ist. Für eine schnelle Umstellung ist die Umstellung von DNS-Einträgen ungeeignet.

Umstellung des(der) MX-Eintrages(Einträge) für die entsprechende Domain

MX-Eintrag nicht ändern, sondern nur den DNS-Eintrag für den Mail-Server auf die neue IP-Nummer stellen. Bedenken Sie auch hier, dass Änderungen im DNS nicht sofort für alle sendenden Hosts wirksam sind.

Achten Sie darauf, dass auch ausgehende Mails über SPONTS versendet werden. Üblicherweise wird für ausgehende Mail nicht der MX-Eintrag verwendet, so dass Sie sicherstellen müssen, dass Clients für ausgehende Mail auch SPONTS verwenden.

Umstellen IP

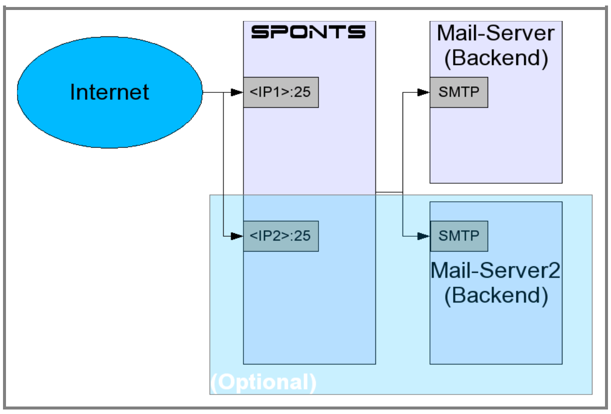


Abbildung 32: Szenario Umstellung IP, DNS oder MX

Hierfür müssen Sie für SPONTS die IP-Nummer des ursprünglichen Mailservers (Backend) verwenden und dem Backend eine andere IP-Nummer geben. Diese

Variante ist sofort einsatzbereit, da alle neuen Zugriffe (eingehende Mails) direkt auf SPONTS erfolgen.

Port-Forwarder auf SPONTS

Bei diesem Szenario werden alle eingehenden Verbindungen auf Port 25 auf TCP-Ebene auf SPONTS umgeleitet. Dies geschieht durch sogenanntes 'Destination NAT' ('DNAT'), bei dem die Zieladresse der eingehenden IP-Pakete für diese Verbindungen umgeschrieben wird. Achten Sie aber unbedingt darauf, dass an dieser Stelle kein 'Source NAT' ('SNAT') (Umschreiben der Quelladresse) stattfindet, da die Quelladresse zur Erfüllung der TKÜV benötigt wird. Aus diesem Grund können Sie hier auch keinen TCP-Proxy einsetzen, da auch hier die Quelladresse geändert wird.

Sie müssen außerdem darauf achten, dass SPONTS über eine funktionierende Internetverbindung verfügt, da eingehende TCP-Verbindungen beantwortet werden müssen. Falls SPONTS in einem privaten IP-Adressbereich liegt, müssen die Antwortpakete des SPONTS (im Gegensatz zu den eingehenden Paketen) per SNAT bzw. Masquerading umgeschrieben werden.

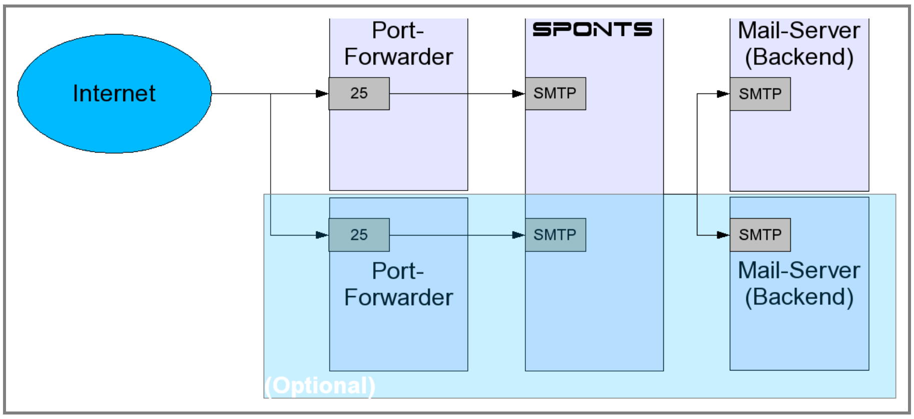


Abbildung 33: Szenario Port-Forwarder

Der Port-Forwarder kann auf dem ursprünglichen Mailserver oder auf einem eigenen Rechner eingerichtet werden oder in einer bereits vorhandenen Firewall eingetragen werden. Falls Port-Forwarder und Backend auf einem Rechner liegen, benötigen Sie für die Verbindungen von SPONTS auf das Backend eine eigene IP-Adresse oder einen gesonderten Port. In diesem Beispiel wird von einem eigenen Port ausgegangen, da diese Variante flexibler ist.

Beispiel für einen Port-Forwarder

Wenn Sie als Betriebssystem Linux 2.4/2.6 mit iptables verwenden, kann der Portforwarder beispielsweise folgendermaßen eingetragen werden:

```
iptables -t nat -A PREROUTING -d <origip> -p tcp --dport 25 -j DNAT
--to-destination <spontsip> <spontsport>
```

Wobei hier gilt:

- <origip>: IP-Adresse, auf die eingehende SMTP-Verbindungen kommen (MX)
- <spontsip>: IP-Adresse des SPONTS
- <spontsport>: Portnummer des SPONTS für SMTP

Sie müssen für das Weiterleiten der IP-Pakete auch noch IP-Routing aktivieren:

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

Wenn Sie den Port-Forwarder auch als Default-Gateway für ausgehende Verbindungen verwenden, müssen Sie mit folgendem Befehl SNAT aktivieren:

```
iptables -t nat -A POSTROUTING -s <spontsip> -p tcp --sport
<spontsport> -j MASQUERADE
```

Achten Sie aber darauf, dass Sie diese Änderungen in die entsprechenden Start-Skripte des Linux-Servers eintragen, damit diese Einstellungen bei einem Neustart nicht verloren gehen.

Sandwich-Technik

Bei der Sandwich-Technik wird der vorhandene Mailserver auf einen anderen Port gelegt. Zusätzlich wird ein weiterer SMTP-Server eingerichtet, der E-Mails auf Port 25 entgegennimmt und diese wiederum per SMTP an SPONTS weiterleitet.
Dazu wird der bereits vorhandene Mailserver in zwei Instanzen aufgeteilt: Eine Instanz nimmt E-Mails per SMTP auf Port 25 aus dem Internet entgegen und führt dabei auch die Access-Kontrolle aus. Diese Instanz leitet die eingehenden E-Mails dann an SPONTS weiter. SPONTS sendet dann wiederum die E-Mail an die zweite Instanz des Mailservers, die die E-Mail dann ausliefert oder weiterleitet. Diese Funktionalität kann mit den wichtigsten Unix-Mailservern erreicht werden.

Bitte beachten Sie, dass die Sandwich-Technik beim Betrieb von SPONTS/Monitor nur dann zulässig ist, wenn das umschließende Mail-System das Durchreichen von SMTP-AUTH beherrscht.

Für TKÜV wird die IP-Adresse des absendenden Hosts benötigt. Da im Sandwich-Modus alle Mails vom vorhandenen Mailserver kommen, kann nicht die IP-Adresse der SMTP-Verbindung ausgewertet werden. Stattdessen werden die „Received“-Kopfzeilen der E-Mail ausgewertet. Achten Sie darauf, dass ihr Mailserver Received-Header erzeugt. Im SPONTS stellen Sie dann über die Option 'Anzahl vorgeschalteter Mailserver im Sandwich-Mode' (S. 54) ein, welche Received-Header er auswerten soll. Ist nur ein Server vorgeschaltet, so stellen Sie „1“ ein. Befinden sich mehrere SMTP-Server vor dem SPONTS, beispielsweise ein Postfix und ein Virenscanner, die beide Received-Header einbauen, so tragen Sie die entsprechende Anzahl der Mailserver ein.

Wenn Sie nicht genau wissen, wie viele Mailserver sich vor dem SPONTS befinden, senden Sie eine Mail von „außen“, beispielsweise über einen Web-Mailer, an eine interne Mailadresse. Lassen Sie sich dann die Kopfzeilen der Mail anzeigen. Eine solche Zeile sieht beispielsweise so aus:

```
Received:from sponts.iku-ag.de (sponts.iku-ag.de [192.168.1.20])
         by h216.loc0.iku-netz.de (Postfix)
         with SMTP id 0C4F01851A1
         for <k.huwig@iku-ag.de>;
         Mon, 17 Jan 2005 11:37:39 +0100 (CET)
```

Hier wird ein Beispiel für den gängigen Mailserver 'postfix' aufgezeigt.

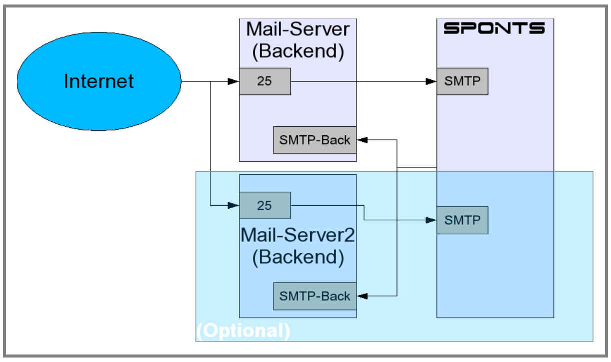


Abbildung 34: Sandwich-Technik für SMTP

Konfigurationsbeispiel für Postfix (z.B. für Debian, SLOX oder SLES)

Um die zwei Instanzen des Postfix zu starten, sind zwei Einträge (Zeilen) in der Datei
`/etc/postfix/master.cf` nötig. Zunächst ändern Sie die Konfiguration des smtpd, der auf Port 25 auf eingehende Verbindungen wartet so, dass er alle Mail an SPONTS weiterleitet:

```
smtp       inet    n    -    n    -    -    smtpd -o
smtpd_proxy_filter=<sponts-ip>:<sponts-port> -o
smtpd_client_connection_count_limit=1000
```

Beachten Sie, dass Sie diese Zeile nicht einfach hinzufügen, sondern die Zeile ergänzen, die mit 'smtp' beginnt. Fügen Sie keine Zeilenumbrüche ein, es muss sich um *eine* Zeile handeln! Fügen Sie dazu einfach die zusätzlichen Optionen (alles hinten '-o') für den Prozess smtpd hinzu. Ersetzen Sie hierbei auch die folgenden Felder:

<sponts-ip>: IP-Adresse oder DNS-Name des SPONTS

<sponts-port>: Port, auf dem SPONTS auf eingehende SMTP-Verbindungen dieses Mailservers wartet

Um die zweite Instanz (für den Backend-Dienst) zu aktivieren, fügen Sie bitte folgende Zeile in die Datei /etc/postfix/master.cf *hinzu*:

```
10026     inet   n       -       n       -       -       smtpd -o
smtpd_authorized_xforward_hosts=127.0.0.1/8 -o
smtpd_client_restrictions= -o smtpd_helo_restrictions= -o
smtpd_sender_restrictions= -o
smtpd_recipient_restrictions=permit_mynetworks,reject -o
smtpd_data_restrictions= -o mynetworks=<sponts-ip>/32 -o
receive_override_options=no_unknown_recipient_checks
```

Diese Zeile konfiguriert den Backend-Dienst auf Port 10026. Falls dieser Port schon belegt ist, können Sie einen beliebigen anderen noch freien Port verwenden. Achten Sie darauf, dass Sie diesen dann auch in der Backendkonfiguration des SPONTS angeben. Ersetzen Sie auch hier <sponts-ip> durch die IP-Nummer oder den DNS-Namen des SPONTS.

Einstellungen im SPONTS

SPONTS kann für beliebig viele Domains und Backends konfiguriert werden. Die Konfiguration ist in zwei Bereiche aufgeteilt:

- Grundkonfiguration für den ersten SMTP Proxy

- Konfiguration weiterer Proxies (ab dem 2. Proxy)

Grundkonfiguration für den ersten SMTP Proxy

Die Grundeinstellungen finden Sie nach dem Anmelden als 'Admin' an der Web-GUI unter 'SPONTS'.

Hier sind folgende Parameter relevant (vgl. 7.2.9 Backend-Servername, S. 49):

Menüpunkt: '*SPONTS → Einstellungen → Versand → Backend*'

- Backend Hostname
- Backend SMTP Portnummer

Tragen Sie bei 'Servername des Backends' und 'SMTP-Portnummer des Backends' die IP-Nummer oder den DNS-Namen sowie den SMTP-Port des Backends ein.

Menüpunkt: '*SPONTS → Einstellungen → Weitergabe*'

- Servername für Backend-Check (vgl. 7.2.8 Weitergabe, S.47)
- SMTP Portnummer für Backendcheck

Bei eingehenden SMTP-Verbindungen wird geprüft, ob das Backend E-Mails für den jeweiligen Empfänger entgegennimmt. Falls hierfür ein anderer Rechner als das Backend verwendet wird, können Sie diesen hier angeben. Bleiben die Felder leer, wird das Backend zur Prüfung der Empfänger benutzt.

- Backend-Check aktivieren

Sie können die Prüfung des Backends auch deaktivieren, was z.B. bei einem MS-Exchange Server sinnvoll ist, da er ohnehin alle E-Mails per SMTP zunächst annimmt.

- Empfänger-Überprüfung über SQL aktivieren

Wenn Sie diesen Check deaktivieren, wird eine Prüfung auf gültige Empfänger und Domains nur gegen das Backend durchgeführt. Die Einstellungen bei 'Empfänger' und 'Lokale Domains' haben dann keine Wirkung mehr.

> Stellen Sie sicher, dass Sie hiermit kein offenes Mail-Relay erzeugen! Dies kann dann passieren, wenn Ihr Backend sämtliche E-Mails von der SPONTS-IP weiterleitet.

Menüpunkt: '*SPONTS → Einstellungen → Versand*'

- Smarthost Servername
- Smarthost SMTP Portnummer

Hier können Sie einen sogenannten 'Smarthost' angeben, an den alle ausgehende Mail geschickt wird. Wenn Sie diese Felder leer lassen, werden ausgehende E-Mails direkt an den zuständigen MX des Empfängers geschickt.

Konfiguration weiterer Proxies (ab dem 2. Proxy)

Um weitere SMTP-Proxies (z.B. für weitere Backends) zu konfigurieren, benutzen Sie die entsprechende Konfigurationsseite unter '*SPONTS → Tabellen → Proxies*' (vgl. 7.3.9 Proxies, S.61). Dort wird Ihnen eine evtl. bereits vorhandene Konfiguration angezeigt. Durch klicken auf 'neuer Eintrag' können Sie einen weiteren Proxy hinzufügen:

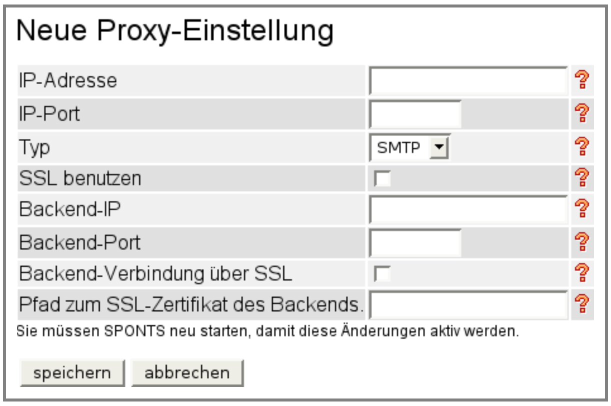


Abbildung 35 Neue Proxy-Einstellungen

- IP-Adresse und IP Port: Stellen Sie hier die IP-Nummer und den Port ein, auf dem SPONTS auf eingehende E-Mails per SMTP lauscht. Wenn Sie das Feld für die IP-Nummer leer lassen, läuft der Dienst auf allen Netzwerkinterfaces des SPONTS.

Achten Sie darauf, dass SPONTS, wenn er direkt als MX angesprochen werden soll, auf Port 25 (SMTP) erreichbar sein muss. Wenn Sie hier also einen anderen Port als 25 einstellen, muss der Zielport umgeschrieben werden. Dies funktioniert nur mit den Methoden Port-Forwarder und Sandwich-Technik.

- Typ: SMTP
- SSL benutzen: Hiermit arbeitet der Port im SSL-Modus. Dies ist sinnvoll, wenn Sie Authentifizierung verwenden.
- Backend IP und Backend Port: Stellen Sie hier IP-Nummer und Port des Backends für diesen Proxy ein.
- Backend-Verbindung über SSL: Hier können Sie einstellen, ob SPONTS versucht, das Backend über SSL anzusprechen. Stellen Sie in diesem Fall bitte sicher, dass Ihr Backend auch SSL unterstützt und der Port stimmt (üblicherweise 995 für POP3/S und 993 für IMAP/S). Im Zweifel sollten Sie SSL komplett deaktivieren.

Mit 'speichern' werden diese Einstellungen gespeichert. Zum Aktivieren müssen Sie SPONTS neu starten.

14.3.3 POP3/IMAP Proxy

Die folgenden Hinweise beziehen sich auf den Betrieb von SPONTS als POP3 bzw. IMAP-**Proxy**. Für den Betrieb als eigenständigen POP3-**Server** (ohne Backend) lesen die bitte Abschnitt 14.3.4 POP3-Betrieb, Seite 110.

Umstellung Netzwerkinfrastruktur für eingehende Verbindungen

POP3 und IMAP können für diese Szenarien identisch behandelt werden, da sie identische Kommunikationswege verwenden (TCP-Verbindung vom Client auf den entsprechenden Port des Mailservers). Dies gilt auch für POP/IMAP über SSL.

Umstellen DNS

In diesem Szenario finden die Zugriffe für IMAP und POP3 direkt auf SPONTS statt. Ziel ist es hier, dass der Client sich beim POP/IMAP-Abruf direkt mit SPONTS

verbindet. SPONTS muss aber für jede dieser Möglichkeiten aus dem Internet auf den entsprechenden Ports für POP/IMAP erreichbar sein.

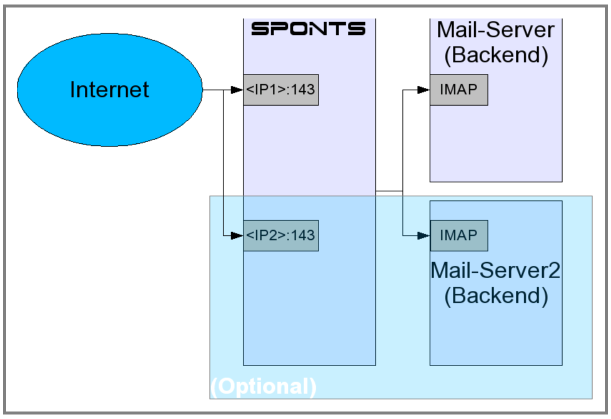


Abbildung 36: Szenario Umstellung IP oder DNS

DNS-Eintrag für den Mail-Server auf die neue IP-Nummer stellen. Bedenken Sie auch hier, dass Änderungen im DNS nicht sofort für alle Clients wirksam sind.

Umstellen IP

Hierfür müssen Sie für SPONTS die IP-Nummer des ursprünglichen Mailservers (Backend) verwenden und dem Backend eine andere IP-Nummer geben. Diese Variante ist sofort einsatzbereit, da alle neuen Zugriffe dann direkt auf SPONTS erfolgen.

Port-Forwarder auf SPONTS

Bei diesem Szenario werden alle eingehenden Verbindungen auf die Ports für POP/IMAP auf TCP-Ebene auf SPONTS umgeleitet. Dies geschieht durch sogenanntes 'Destination NAT', bei dem die Zieladresse der eingehenden IP-Pakete für diese Verbindungen umgeschrieben wird. Achten Sie aber unbedingt darauf, dass Sie an dieser Stelle kein SNAT (Umschreiben der Quelladresse) stattfindet, da die Quelladresse zur Erfüllung der TKÜV benötigt wird. Aus diesem Grund können Sie hier auch keinen TCP-Proxy einsetzen, da auch hier die Quelladresse geändert wird.

Sie müssen außerdem darauf achten, dass das Backend über eine funktionierende Internetverbindung verfügt, da eingehende TCP-Verbindungen beantwortet werden müssen. Falls das Backend in einem privaten IP-Adressbereich liegt, müssen die Antwortpakete des Mailservers (im Gegensatz zu den eingehenden Paketen) per SNAT bzw. Masquerading umgeschrieben werden.

Der Port-Forwarder kann auf dem ursprünglichen Mailserver oder auf einem eigenen Rechner eingerichtet werden oder in einer bereits vorhandenen Firewall eingetragen werden.

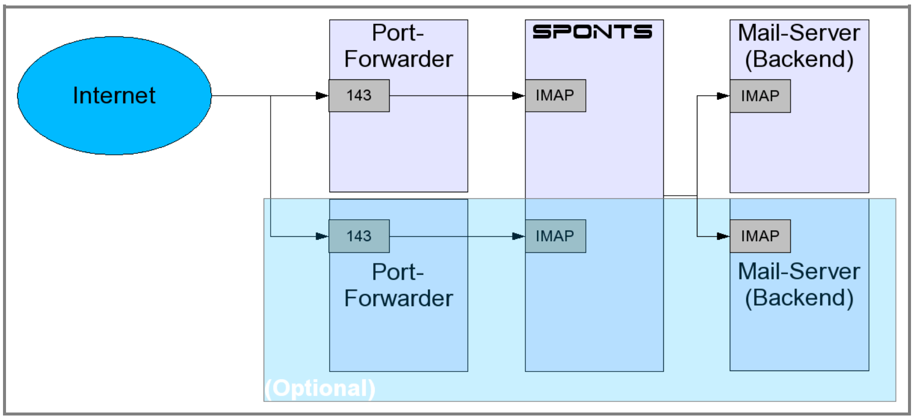


Abbildung 37: Szenario Port-Forwarder

Beispiel für einen Port-Forwarder

Dieses Beispiel gilt für POP3, für IMAP muss nur die Portnummer 143 statt 110 verwendet werden.

Wenn Sie als Betriebssystem Linux 2.4/2.6 mit iptables verwenden, kann der Portforwarder beispielsweise folgendermaßen eingetragen werden:

```
iptables -t nat -A PREROUTING -d <orig-ip> -p tcp --dport 110 -j
DNAT --to-destination <sponts-ip>:<sponts-port>
```

Wobei hier gilt:

- <orig-ip>: IP-Adresse, auf die eingehende POP3-Verbindungen kommen
- <sponts-ip>: IP-Adresse des SPONTS
- <sponts-port>: Portnummer des SPONTS für POP3

Sie müssen für das Weiterleiten der IP-Pakete auch noch IP-Routing aktivieren:

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

Falls Sie noch SNAT für ausgehende Pakete aktivieren wollen, kann das mit folgendem Befehl geschehen:

```
iptables -t nat -A POSTROUTING -s <sponts-ip> -p tcp --sport
<sponts-port> -j MASQUERADE
```

Achten Sie aber darauf, dass Sie diese Änderungen in die entsprechenden Start-Skripte des Linux-Servers eintragen, damit diese Einstellungen bei einem Neustart nicht verloren gehen.

Einstellungen im SPONTS

SPONTS kann für quasi beliebig viele Domains und Backends konfiguriert werden. Die Konfiguration ist in zwei Bereiche aufgeteilt:

- Grundkonfiguration für den ersten POP3 Proxy
- Konfiguration weiterer Proxies (ab dem 2. Proxy)

Grundkonfiguration für den ersten POP3 Proxy

Die Grundeinstellungen finden Sie nach dem Anmelden als 'Admin' an der Web-GUI unter dem Menüpunkt *'SPONTS → Einstellungen → Monitor'* *(vgl. 7.2.12 Monitor, S. 53)*.

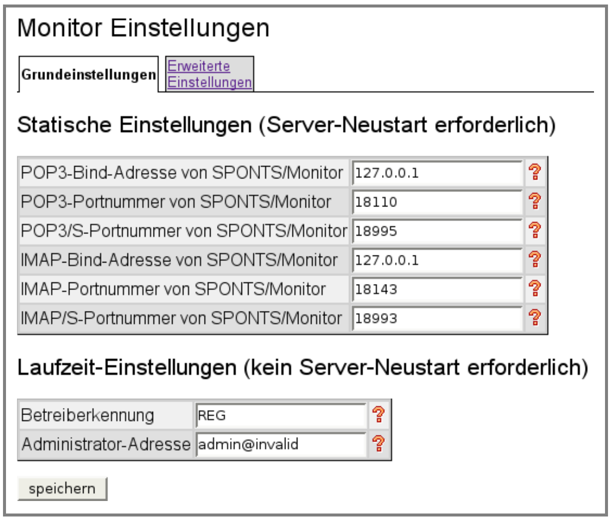


Abbildung 38: Einrichtung POP3- und IMAP-Proxy

Hier können Sie die Parameter für eingehende Verbindungen auf SPONTS konfigurieren. Sie sollten hier die Standard-Ports für IMAP und POP3 verwenden, wie im Beispiel gezeigt. Wenn Sie die Felder für 'Bind-Adresse' leer lassen, wartet SPONTS auf allen Netzwerkinterfaces auf eingehende Verbindungen.

Das Backend stellen Sie unter *'SPONTS → Einstellungen→ Monitor → POP3'*(vgl. 7.2.12 Monitor – POP3, S. 54) und *'SPONTS → Einstellungen→ Monitor→ IMAP*'(vgl. 7.2.12 Monitor – IMAP, S. 54):

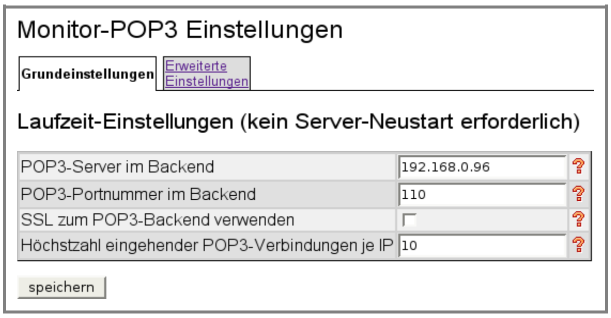


Abbildung 39: Einrichten POP3-Backend

Folgende Parameter sind hier wichtig:

- 'POP3-Server im Backend' und 'POP3-Portnummer im Backend': Hostname/IP-Adresse des POP3 Backends

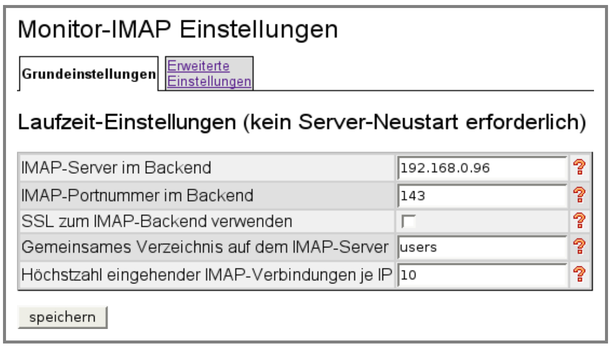


Abbildung 40Einrichtung IMAP-Backend

- 'IMAP-Server im Backend' und 'IMAP-Portnummer im Backend': Hostname/IP-Adresse des IMAP Backends

Konfiguration weiterer Proxies (ab dem 2. Proxy)

Um weitere SMTP-Proxies (z.B. für weitere Backends) zu konfigurieren, benutzen Sie die entsprechende Konfigurationsseite unter '*SPONTS → Tabellen → Proxies*' (vgl. 7.3.9 Proxies, S.61). Dort wird Ihnen eine evtl. bereits vorhandene Konfiguration angezeigt. Durch klicken auf '*neuer Eintrag*' können Sie einen weiteren Proxy hinzufügen:

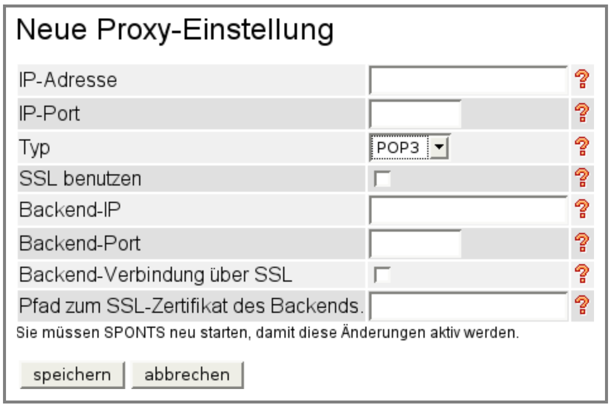


Abbildung 41: Einrichtung weiterer POP3-Proxies

IP address und IP port: Stellen Sie hier die IP-Nummer und den Port ein, auf dem SPONTS auf eingehende POP3-Verbindungen lauscht. Wenn Sie das Feld für die IP-Nummer leer lassen, läuft der Dienst auf allen Netzwerkinterfaces des SPONTS.

- Typ: POP3 (oder IMAP)
- SSL benutzen: Hiermit erlauben Sie SSL und TLS-Verbindungen auf den SPONTS.
- Backend IP und Backend Port: Stellen Sie hier IP-Nummer und Port des Backends für diesen Proxy ein.
- Backend-Verbindung über SSL: Hier können Sie einstellen, ob SPONTS versucht, das Backend per SSL anzusprechen. Stellen Sie in diesem Fall bitte sicher, dass Ihr Backend auch SSL unterstützt. Im Zweifel sollten Sie SSL komplett deaktivieren.

Mit '*speichern*' werden diese Einstellungen gespeichert. Zum Aktivieren müssen Sie SPONTS neu starten.

14.3.4 POP3-Betrieb

SPONTS als POP3-Server

Der Benutzer-Zugriff auf die Warteschlange ermöglicht den Betrieb von SPONTS als vollwertigen POP3-Server (ohne SMTP-Backend). Über die entsprechende Einstellung in der Rubrik 'UMS' kann die POP3-Zugriffs-Möglichkeit für Benutzer jederzeit aktiviert bzw. deaktiviert werden.

Der Administrator trägt die Email-Adressen, für die ein POP3-Konto eingerichtet werden soll, in der Tabelle 'Benutzer' ein, legt ein Passwort fest und teilt es dem

Benutzer mit. Der Benutzer kann seine Emails mit einem beliebigen POP3-Client abrufen.

Automatisierter Abruf externer POP3-Konten

SPONTS kann in regelmäßigen Abständen externe POP3-Konten abrufen und an einstellbare Empfänger-Adressen weiterleiten. Verwenden Sie die dazu die Tabelle 'Abrufkonten', siehe Abschnitt 7.3.3 Abrufkonten (POP3).

14.4 Administration

Die Administration erfolgt ausschließlich über die Web-GUI. Hierbei werden - wie von TKÜV §16 gefordert - alle relevanten Aktionen protokolliert. Deshalb verfügt SPONTS/Monitor über eine eigene Benutzerverwaltung. Diese kennt 3 verschiedene Benutzer-Rollen:

1. Sysadmin: darf Benutzer anlegen, ändern, löschen und Rechte vergeben
2. Operator: darf Überwachungsmaßnahmen anlegen, einsehen, verlängern und löschen
3. Inspector: prüft und löscht Protokolldateien

Beim Setzen der Passwörter mit 'setup' wird ein Sysadmin mit Login 'admin' und dem für 'admin' gewählten Passwort angelegt. Mit diesem Zugang können weitere Benutzer angelegt werden.

14.4.1 Anmeldung

Die Web-Oberfläche ist standardmäßig erreichbar unter:
https://<ip-adresse>:8443/monitor/ (verschlüsselt)

Geben Sie in dem Dialog Ihre Zugangsdaten ein:

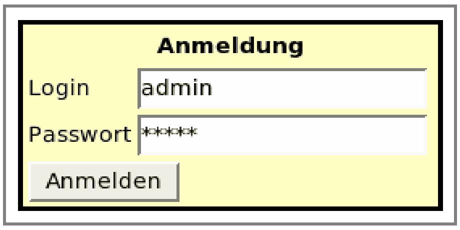


Abbildung 42: Anmeldung an SPONTS/Monitor

Im Auslieferungszustand ist das Adminstratorpasswort 'start'.

Klicken Sie dann auf 'Anmelden'

14.4.2 Anmeldung über verschlüsselten Tunnel

Die Verbindung zum SPONTS/Monitor muss über das firmeneigene Netzwerk oder über eine verschlüsselte Punkt-zu-Punkt-Verbindung erfolgen. Eine verschlüsselte Punkt-zu-Punkt-Verbindung können Sie mit SSH erzeugen:

```
ssh -N -L 8443:localhost:8443 benutzer@sponts
```

Mit dem unter Windows verfügbaren Programm PuTTY geht dies, indem Sie unter 'SSH - Tunnels' einen Port-Forwarder einrichten:

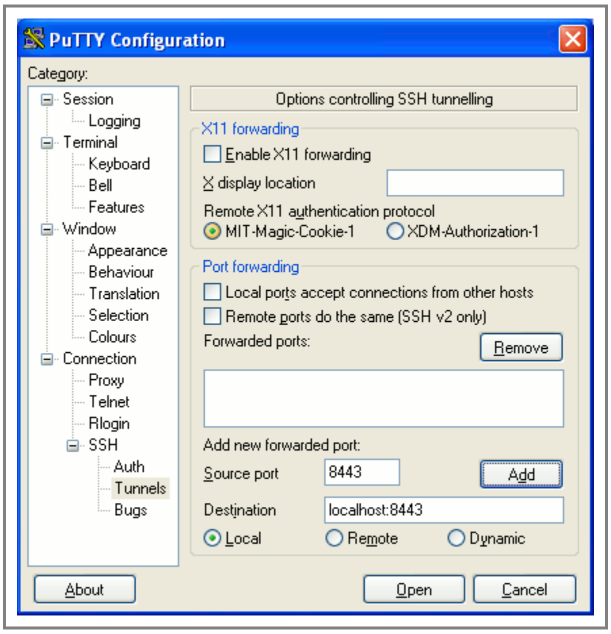


Abbildung 43 Port-Forwarder mit PuTTY

und auf 'Add' klicken:

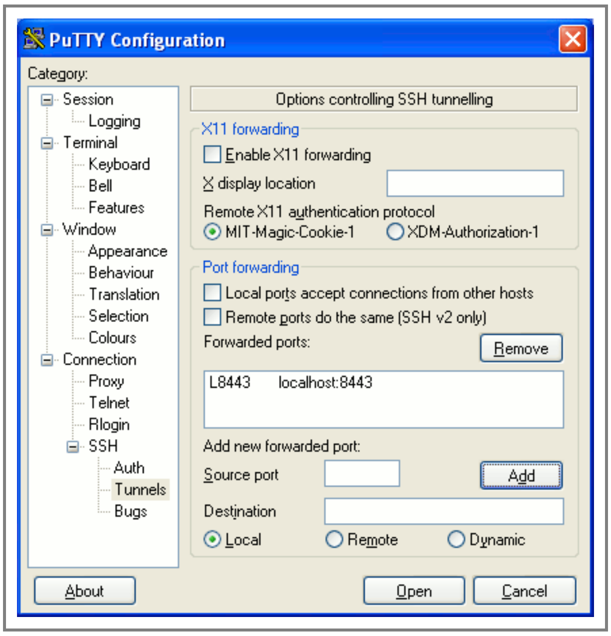


Abbildung 44 eingerichteter Port-Forwarder mit PuTTY

Danach können Sie in Ihrem Browser über

```
https://localhost:8443/
```

auf die normale SPONTS-GUI und über

```
https://localhost:8443/monitor/
```

auf die SPONTS/Monitor-GUI zugreifen.

14.4.3 Benutzerverwaltung

Die Benutzerverwaltung ist nur für Benutzer mit der Rolle 'System-Administrator' möglich. Diese erhalten folgendes Menu:



Abbildung 45: Benutzermenü

In der Mitte befindet sich eine Liste aller SPONTS/Monitor-Benutzer mit zugehörigen Aktionen und links ein Menu für weitere Aktionen.

Benutzer anlegen

Klicken Sie links auf 'Benutzer anlegen' und geben Sie die entsprechenden Daten ein. Klicken Sie dann auf 'Benutzer anlegen' zum Anlegen des Benutzers oder auf 'Abbrechen' zum Abbrechen der Eingabe.

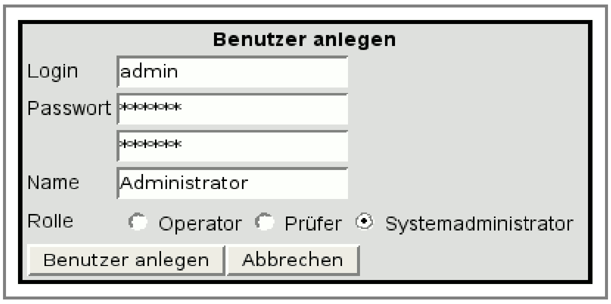


Abbildung 46: Benutzer anlegen

Das eingegebene Passwort muss der Benutzer beim ersten Anmelden ändern. Das Anlegen von Benutzern wird protokolliert.

Benutzer bearbeiten

Klicken Sie auf den Link 'bearbeiten' hinter dem entsprechenden Benutzer.

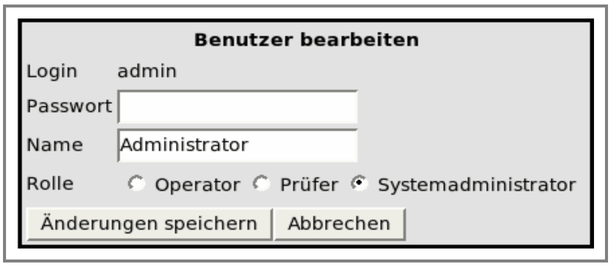


Abbildung 47: Benutzer bearbeiten

Geben Sie die geänderten Daten ein und klicken Sie auf 'Änderungen speichern' zum Speichern oder auf 'Abbrechen' zum Abbrechen. Das eingegebene Passwort

muss der Benutzer beim ersten Anmelden ändern. Wenn Sie die Rolle eines Benutzers ändern, so wird dies protokolliert.

Benutzer löschen

Klicken Sie auf den Link 'löschen' hinter dem entsprechenden Benutzer.



Abbildung 48: Benutzer löschen

Klicken Sie auf 'Benutzer löschen', um ihn zu löschen oder auf 'Abbrechen' zum Abbrechen. Wenn Sie einen Benutzer löschen, so wird dies protokolliert.

Passwort ändern

Jeder Benutzer muss nach seiner ersten Anmeldung sein Passwort ändern, damit der Systemadministrator dieses Passwort nicht kennt. Er kann sein Passwort auch jederzeit durch Klicken auf 'Passwort ändern' ändern.

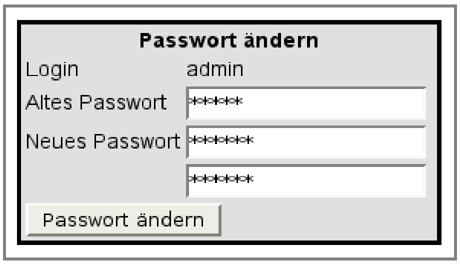


Abbildung 49 Passwort ändern

Das neue Passwort muss anders als das alte Passwort lauten. Die Änderung des Passwortes wird protokolliert.

14.4.4 Überwachungsmaßnahmen (ÜM) verwalten

Die Verwaltung von ÜM ist nur für Benutzer mit der Rolle 'Operator' möglich. Diese erhalten folgendes Menu:

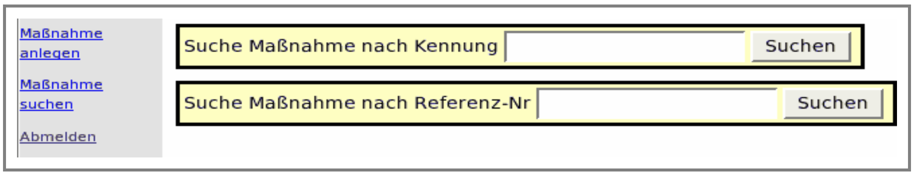


Abbildung 50: Überwachungsmaßnahmen Menu

In der Mitte befinden sich zwei Felder für die Eingabe von Suchkriterien und links ein Menu für weitere Aktionen.

Überwachungsmaßnahmen anlegen

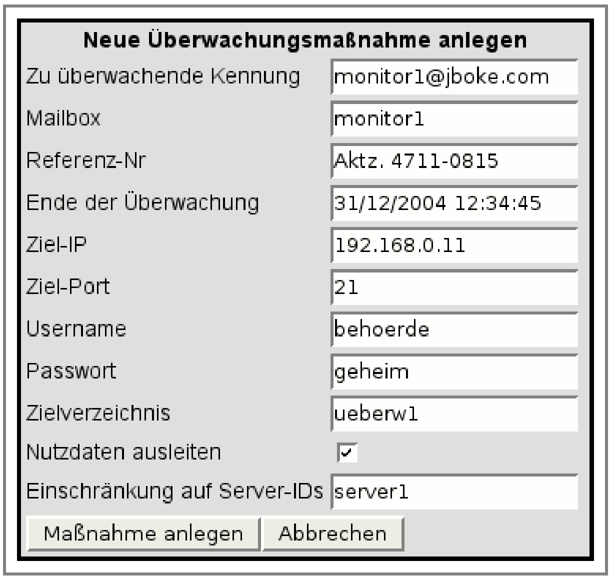


Abbildung 51: Überwachungsmaßnahme anlegen

Klicken Sie links auf 'Maßnahme anlegen' und geben Sie die entsprechenden Daten ein. Klicken Sie dann auf 'Maßnahme anlegen' zum Anlegen der Maßnahme oder auf 'Abbrechen' zum Abbrechen der Eingabe.

'Mailbox' bezieht sich auf den SMTP-AUTH/POP3/IMAP-Login des zu Überwachenden. 'Ziel-IP','Ziel-Port', 'Username', 'Passwort' und 'Zielverzeichnis' beziehen sich auf den FTP-Server der berechtigten Stelle. Das Ende der Maßnahme darf maximal 3 Monate nach dem aktuellen Datum liegen. Das Anlegen von Überwachungsmaßnahmen wird protokolliert.

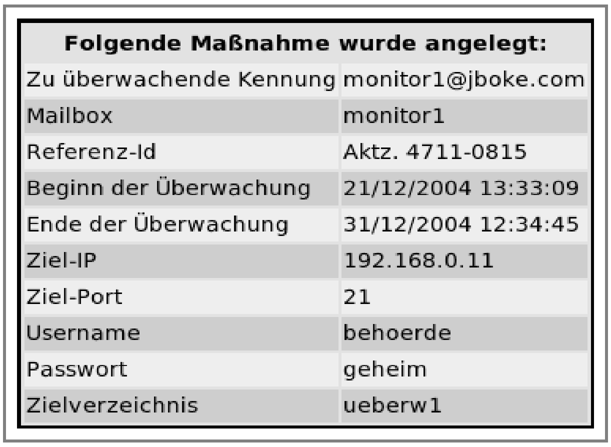


Abbildung 52: Bestätigung einer angelegten Überwachungsmaßnahme

Wurde die Überwachungsmaßnahme erfolgreich angelegt, so erscheint der folgende Dialog, der die Daten der Überwachungsmaßnahme enthält. Prüfen Sie genau, ob die Daten der Überwachungsverfügung entsprechen!

Überwachungsmaßnahme suchen

Klicken Sie links auf 'Maßnahme suchen'. Sie können nach überwachter Kennung oder Referenz-Nr suchen. Nach einen Klick auf den entsprechenden 'Suchen'-Knopf erscheinen alle entsprechenden Maßnahmen.

Zu überw. Kennung	Mailbox	Zuordnungsnummer	
monitor1@jboke.com	monitor1	Aktz. 4711-0815	ansehen löschen

Abbildung 53: Suchergebnis Überwachungsmaßnahme

Überwachungsmaßnahme ansehen

Überwachungsmaßnahme	
Zu überwachende Kennung	monitor1@jboke.com
Mailbox	monitor1
Referenz-Id	Aktz. 4711-0815
Beginn der Überwachung	21/12/2004 13:33:09
Ende der Überwachung	31/12/2004 12:34:45
Ziel-IP	192.168.0.11
Ziel-Port	21
Username	behoerde
Passwort	geheim
Zielverzeichnis	ueberw1
Maßnahme verlängern	Abbrechen

Abbildung 54: Überwachungsmaßnahme ansehen

Klicken Sie auf den Link 'ansehen' hinter einer Überwachungsmaßnahme, um diese anzusehen.

Das Ansehen von Überwachungsmaßnahmen wird protokolliert.

Verlängern von Überwachungsmaßnahmen

In der Anzeige einer Überwachungsmaßnahme können Sie ein anderes Ende eintragen und dann auf 'Maßnahme verlängern' klicken. Damit wird die Maßnahme verlängert. Eine Maßnahme darf maximal um 3 Monate verlängert werden. Das Verlängern von Maßnahmen wird protokolliert.

Löschen von Überwachungsmaßnahmen

Klicken Sie auf den Link 'löschen' hinter der entsprechenden Maßnahme.

Folgende Maßnahme wirklich löschen?	
Zu überwachende Kennung	monitor1@jboke.com
Mailbox	monitor1
Referenz-Id	Aktz. 4711-0815
Maßnahme löschen	Abbrechen

Abbildung 55: Überwachungsmaßnahme löschen

Klicken Sie auf 'Maßnahme löschen', um sie zu löschen oder auf 'Abbrechen' zum Abbrechen. Wenn Sie eine Maßnahme löschen, so wird dies protokolliert.

14.4.5 Prüfung

Die Prüfung von Operatorlogs ist nur für Benutzer mit der Rolle 'Prüfer' möglich.

Operatorlogs prüfen

Mindestens alle 3 Monate müssen die Logdateien des Operators geprüft werden. Hierbei ist die Logdatei mit den vorliegenden Überwachungsverfügungen zu vergleichen.

> Insbesondere ist hierbei darauf zu achten, dass zu jeder ÜM auch eine entsprechende schriftliche Verfügung existiert. Besteht eine besondere Dringlichkeit, so dürfen Überwachungsverfügungen vorab per Fax übermittelt werden. Binnen 7 Tagen muss eine schriftliche Ausfertigung folgen. Geschieht dies nicht, so ist die ÜM zu löschen (siehe auch TKÜV §12 (2)).

Als Prüfer erhalten Sie eine Liste aller Logeinträge, die durch Aktionen eines der Operatoren verursacht worden sind. Diese enthalten:

- eine fortlaufende Nummerierung (Id)
- die eindeutige Nummer der ÜM
- die zu überwachenden Kennung
- Beginn und Ende der Überwachung
- Ziel-IP für die auszuleitenden Daten
- Name des Operators, der diese Aktion ausgeführt hat

Danach kommt eine Spalte, die angibt, ob dieser Eintrag bereits geprüft worden ist. Ist er noch nicht geprüft, so erscheint ein Link „als geprüft markieren“, ansonsten erscheint der Text „geprüft“.

Gleichen Sie jeden Eintrag in der Logdatei mit den schriftlichen Verfügungen ab. Sie können hierbei die Sortierung der Logeinträge über zwei Links oberhalb der Liste nach zu überwachender Kennung oder nach Zeitpunkt der Aktion sortieren. Gibt es Umstimmigkeiten, so sind diese dem Operator mitzuteilen und umgehend zu beheben. Die Unstimmigkeiten sind an die RegTP zu melden (TKÜV §17 (2)). Gibt es keine Unstimmigkeiten, so ist dies ebenfalls formlos an die RegTP zu melden.

Datensätze, die geprüft worden sind werden durch Anwahl des Links „als geprüft markieren“ entsprechend markiert.

Operatorlogs löschen

Nach einer Prüfung sind die Logeinträge noch in dem Quartal, das dem Ende der ÜM folgt aufzubewahren und danach zu löschen. Wählen Sie hierzu den Punkt„Protokoll löschen“. Nach einer Sicherheitsabfrage werden alle Logeinträge, die als geprüft markiert sind und deren ÜM lange genug abgelaufen sind, automatisch gelöscht. SPONTS/Monitor löscht nur diejenigen Einträge, die gelöscht werden dürfen, so dass Sie diese Funktion jederzeit auswählen können.

14.5 FTP

Die Daten einer Überwachung werden in XML-Dateien geschrieben und per FTP übermittelt. Hierbei wird 24 Stunden lang versucht, die Datei zu übertragen. Schlägt dies fehl, so wird die Datei in das Verzeichnis 'monitor-orphans' kopiert und der SPONTS-Administrator mit einer E-Mail benachrichtigt. Dieser hat dann entsprechende Schritte einzuleiten.

14.5.1 Ausleitung über Online-Verbindung

Besteht eine direkte Verbindung zur berechtigten Stelle, beispielsweise über eine SINA-Box, so ist beim Anlegen einer Überwachungsmaßnahme der FTP-Server der berechtigten Stelle anzugeben. FTP-Verbindungen vom SPONTS dorthin müssen von Ihrem Netzwerk über die SINA-Box geleitet werden.

14.5.2 Speichern auf Datenträger

Wird das Speichern der Datensätze auf einem Datenträger gewünscht, so benötigen Sie einen eigenen FTP-Server. Geben Sie diesen beim Anlegen einer Überwachungsmaßnahme an, so dass SPONTS die XML-Dateien an diesen Server schickt. Von dort aus können Sie die Datensätze auf den Datenträger übertragen. Schützen Sie den FTP-Server gegen Zugriffe Unbefugter!

14.5.3 FTP-Proxy

SPONTS kann mit einem eigenen FTP-Proxy kommunizieren. Dieser ist in Java geschrieben und damit unter jedem gängigen Betriebssystem lauffähig.

SSL-Zertifikat

Zum Betrieb benötigen Sie ein SSL-Zertifikat. In 4.4 Zertifikate (S. 12) ist beschrieben, wie Sie ein solches erzeugen können. Da die so erzeugten Zertifikate nicht von einer der vom JRE akzeptierten zentralen Zertifizierungsinstanzen unterschrieben wurden, werden sie von der JRE nicht akzeptiert und mit der Fehlermeldung 'certificate_unknown' bzw 'sun.security.validator.ValidatorException: No trusted certificate found' abgewiesen. Deshalb ist es notwendig, die Schlüssel auf beiden Seiten der Verbindung bekannt zu machen. Hierzu muss jeweils ein Schlüsselzertifikat mit Angabe des Keystore-Passwortes exportiert werden:

```
keytool -export -keystore sponts.keystore -file sponts.cer \
        -alias sponts
```

bzw.

```
keytool -export -keystore ftpproxy.keystore \
        -file ftpproxy.cer -alias sponts
```

Auf der jeweils anderen Seite muss der Schlüssel importiert werden, wobei ein eindeutiger Alias verwendet werden muss, damit mehrere Schlüssel unterschieden werden können:

```
keytool -import -keystore ftpproxy.keystore -file sponts.cer \
        -alias schluessel1
```

bzw.

```
keytool -import -keystore sponts.keystore -file ftpproxy.cer \
        -alias schluessel1
```

Werden mehrere SPONTS an einen FTP-Proxy angebunden, so empfiehlt es sich, den Namen des Kunden und eine fortlaufende Nummer für die Box als Alias zu verwenden.

SQL-Datenbank

Außerdem benötigen Sie eine SQL-Datenbank, die Zugangsdaten für den Proxy enthält. Das folgende Beispiel bezieht sich auf eine MySQL-Datenbank, vom Prinzip her kann jede SQL-Datenbank verwendet werden, für die ein JDBC-Treiber verfügbar ist.

Im Folgenden wird von folgenden Daten ausgegangen:

Servername:	mysql.intern.sponts.com
Datenbank:	ftpproxy
Username:	sponts-ftp-user
Passwort:	geheimes-passwort

In dieser Datenbank ist folgende Tabelle anzulegen:

```
CREATE TABLE `ftpuser` (
       `user` varchar(20) NOT NULL default '',
       `password` varchar(20) NOT NULL default '',
       PRIMARY KEY (`user`)
);
```

Der MySQL-Benutzer 'ftpproxy' benötigt nur Leserechte auf dieser Tabelle. In diese Tabelle tragen Sie dann beliebig viele Zugangsdaten für den Proxy ein.

Serverseitige Konfiguration

Zum Starten des Proxies benötigen Sie einen Rechner mit JRE 1.4.2 oder besser. Darauf die Dateien 'FtpProxy.jar', den JDBC-Treiber unter dem Namen 'jdbc.jar' kopieren sowie den Keystore mit dem SSL-Zertifikat kopieren.

Da der JDBC-Treiber automatisch geladen wird, muss die Jar-Datei 'jdbc.jar' heißen, damit sie gefunden wird.

Gestartet wird der Proxy wie folgt:

```
java -jar FtpProxy.jar <port> <jdbc-driver> <jdbc-url> <jdbc-user>
<jdbc-password> <keystore> <keystore-pw> <key-pw> <need trusted
certificate: yes|no>
```

wobei der Port 21000 fest vorgegeben ist, also beispielsweise

```
java -jar FtpProxy.jar \
      21000 \
      org.gjt.mm.mysql.Driver \
      jdbc:mysql://mysql.intern.http.net/ftpproxy \
      sponts-ftp-user \
      geheimes-passwort \
      ftpproxy.keystore \
      geheim-keystore \
      geheim-key \
      no
```

Das ganze sollte so gestartet werden, dass nach einem Absturz der Dienst neu gestartet wird, also beispielsweise unter Linux in die /etc/inittab oder unter Windows als Service eintragen.

Clientseitige Konfiguration (SPONTS)

In den SPONTS-Monitoreinstellungen den DNS-Namen des Proxies sowie Benutzername und Passwort angeben. Wir empfehlen hierbei für jeden SPONTS ein eigenes Login zu verwenden.

Routing

Bei dem Routing des FTP-Proxies ist zu beachten, dass aller Datenverkehr zur SINA-Box gehen muss, bis auf den, der auf Port 21000 reinkommt. Diese muss zu den SPONTS-Boxen zurück geroutet werden, entweder über einzelne Host-Routen oder Port-basierendes Source-Based-Routing.

14.6 Datenbank

Für die SPONTS/Monitor-Einstellungen gibt es eine eigene Datenbank 'spontsmonitor'. Diese dürfen Sie nicht einsehen oder gar verändern, da sowohl das Einsehen, als auch das Verändern von Überwachungsmaßnahmen nur berechtigten Personen erlaubt ist und die Zugriffe protokolliert werden müssen. Direkte Zugriffe auf die Datenbank gehen nicht über den SPONTS und können deshalb nicht protokolliert werden. Deshalb wird hierfür auch ein eigenes zufällig generiertes Passwort verwendet. Sorgen Sie dafür, dass die Settings.properties nicht in falsche Hände gerät, da diese das Passwort enthält!

14.7 Connector

Der Monitor-Connector erlaubt den Zugriff von außen auf die Monitor-Datenbank sowie das Ausleiten von E-Mails.

Er unterstützt verschlüsselte Verbindungen und Authentisierung, ist telnet-kompatibel und auf Performanz optimiert.

14.7.1 Funktionalität

Das Protokoll orientiert sich an gängigen Email-Protokollen (einfache zeilenbasierte Befehle, menschen-lesbar) und bietet folgende Funktionalität:

1. Authentisierung
2. Bestimmung, ob ein Postfach überwacht wird
   - ➔ Parameter: E-Mailadresse, Postfach, Server-ID
   - ➔ Antworten:

   - nicht überwacht
   - überwacht ohne Nutzdaten
   - überwacht mit Nutzdaten
3. Bestimmung, ob eine Mail ausgeleitet werden muss
   - ➔ Parameter: E-Mailadresse, Postfach, Server-ID, Message-ID
   - ➔ Antworten:
     - keine Ausleitung
     - mit Nutzdaten
     - ohne Nutzdaten

14.7.2 Protokoll-Spezifikation

Im folgenden ist grob dargestellt, wie das Protokoll konkret abläuft:

```
< 220 Text <Challenge in spitzen Klammern>

> AUTHENTICATE CRAM-MD5 <client-id> <response> (einmal)
< 235 ok | 535 access denied ( -> disconnect )

-> Filterbeginn

> MAILADDRESS <mailaddress> (beliebig oft)
< 250 ok

> ACCOUNT <account> (beliebig oft)
< 250 ok

> SERVER <serverid> (einmal, optional)
< 250 ok

-> Ausleitungsbeginn

> CHECK [<message-id>]
< 300 unmonitored | 310 monitored without userdata | 320 monitored
with userdata

> PROTOCOL [POP3|IMAP|SMTP|HTTP]
< 250 ok

> PARTNER <partner>
< 250 ok

> DIRECTION [RECEIVED|RETRIEVED|SENT|LEFT]
< 250 ok

> RELEASECAUSE <releasecause>
< 250 ok

> IP <ip>
< 250 ok

> TRANSMIT ( -> Ausleitung ohne Nutzdaten )
< 250 ok

> TRANSMIT {size}
< 354 go ahead
```

```
<size bytes>[{size}CRLF<size bytes>]* CRLF
< 250 ok
```

-> Ausleitungsende

```
> RESET ( -> Ausleitungs- & Filter-Reset )
< 250 ok

> QUIT
< 221 goodbye
```